**IN THE UNITED STATES DISTRICT
COURT FOR THE WESTERN DISTRICT
OF TEXAS AUSTIN DIVISION**

| | |
|---|---|
| GOSECURE, INC.<br>Plaintiff,<br>v.<br>CROWDSTRIKE, INC., and<br>CROWDSTRIKE HOLDINGS, INC.<br>Defendants. | **Case No. 24-cv-526**<br>**JURY TRIAL DEMANDED** |

## COMPLAINT

Plaintiff GoSecure, Inc. ("GoSecure" or "Plaintiff") brings this patent infringement action against Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc. ("CrowdStrike" or "Defendants").

GoSecure began developing innovative behavioral analysis techniques that would become foundational to end-point detection and response information security solutions by no later than 2009, and began seeking patent protection. When GoSecure began seeking patent protection for its inventions, CrowdStrike did not exist. Its founders—Mr. Dmitri Alperovitch and Mr. George Kurtz—each received detailed technical information about GoSecure's patented technology before founding CrowdStrike. Mr. Alperovitch even joined GoSecure's Board of Directors, where he convinced GoSecure to hire one of his acquaintances as a senior engineer, only to hire that same engineer to join CrowdStrike a few months later. In the decade-plus since then, CrowdStrike has used GoSecure's patented technology to generate tens of billions of dollars in revenue at GoSecure's expense.

## NATURE OF THE ACTION

1. This is a civil action for infringement of United States Patent Nos. 9,954,872 ("'872 Patent") and 9,106,697 ("'697 Patent") (collectively, the "Asserted Patents") under the patent laws of the United States, 35 U.S.C. § 1 *et seq*.

## THE PARTIES

2. Plaintiff GoSecure, Inc. is a corporation organized and existing under the laws of the State of Delaware with its principal place of business located at 13220 Evening Creek Dr. S, Suite 107, San Diego, CA 92128. GoSecure has employees located throughout the United States and Canada, including in Austin, Boston, Montreal, and San Diego.

3. GoSecure is the owner of all rights, title, and interest in and to the Asserted Patents. GoSecure has launched multiple cybersecurity products incorporating its patented technology, including, for example, the GoSecure Titan® Platform.[1] GoSecure provides its products to customers who operate throughout the United States and Canada, including within this District.

4. On information and belief, Defendant CrowdStrike Holdings, Inc. is a "Delaware corporation with its principal executive office in Austin."[2] For example, CrowdStrike Holdings, Inc.'s "principal executive offices occupy approximately 47,618 square feet in Austin, Texas."[3]

[1] *See, e.g.*, https://gosecure.ai/wp-content/uploads/GoSecure_Datasheet_Titan-Platform-_2024.pdf (last visited May 15, 2024).

[2] *See, e.g.*, *Webroot, Inc. v. CrowdStrike, Inc.*, Case No. 6:22-cv-00241, Dkt. 59 at 2 (W.D. Tex. Sept. 7, 2022); *see also* https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/ (last visited May 15, 2024).

[3] *See* https://ir.crowdstrike.com/static-files/29e71f45-3c39-4c2c-9159-5e7bb9f3315b (CrowdStrike U.S. Securities and Exchange Commission Form 10-K for Fiscal Year ended January 31, 2024) at 57 (last visited May 15, 2024).

Defendant CrowdStrike Holdings, Inc. is the parent of and directly and wholly owns Defendant CrowdStrike, Inc.[4]

5. On information and belief, Defendant CrowdStrike, Inc. is a "Delaware corporation and maintains multiple offices, including an office in Austin."[5] Defendant CrowdStrike, Inc. is registered with the Secretary of State to conduct business in Texas.

## JURISDICTION AND VENUE

6. The Court has subject matter jurisdiction over these claims under 28 U.S.C. §§ 1331 and 1338(a) and the patent laws of the United States, 35 U.S.C. § 1 *et seq*.

7. The Court has personal jurisdiction over Defendants because they have their principal place of business in this District and regularly conduct business in the State of Texas and in this District. On information and belief, Defendants' business includes operating systems, using software, providing services, and/or engaging in activities in Texas and in this District that infringe one or more claims of the Asserted Patents, as well as inducing and contributing to the direct infringement of others through acts in this District.

8. Defendants have also, directly and through their extensive network of partnerships, including through local IT service providers, purposefully and voluntarily placed infringing security software and services including, but not limited to, the Falcon Platform, Falcon Endpoint Protection, Falcon Exposure Management, Falcon Insight XDR, Falcon ASPM, Threat Graph, Falcon Counter Adversary Operations, Falcon Next-Gen SIEM, Falcon for Defender, Falcon Identity Protection, Falcon for IT, Falcon Foundry, Falcon Data Protection, Falcon Prevent, Falcon Firewall Management, Falcon Adversary OverWatch, Falcon Discover, Falcon Device Control

[4] *See id.* at 71.

[5] *See, e.g., Webroot, Inc. v. CrowdStrike, Inc.*, Case No. 6:22-cv-00241, Dkt. 59 at 2 (W.D. Tex. Sept. 7, 2022).

and Falcon Cloud Security, including prior versions and functionalities that are the same or essentially the same (collectively, "Falcon Platform" or "Accused Products") that practice the methods claimed in the Asserted Patents into the stream of commerce in this District.[6]

9. On information and belief, Defendant CrowdStrike, Inc. has hundreds of employees in this District—including positions in engineering, sales, marketing, and finance.[7]

10. On information and belief, CrowdStrike's employees located in this District have relevant information, including information concerning the products and services Defendants provide and how those products operate.

11. On information and belief, engineers responsible for developing the Accused Products and knowledgeable about the Accused Products are located in Austin, Texas.[8]

12. On information and belief, Mr. Sean Slaton is a "National Sales Director for SMB Sales," is "knowledgeable about CrowdStrike's sales organization and practices," and "lives in Austin and works in CrowdStrike's Austin Office."[9]

13. On information and belief, Mr. Greg Ellet is CrowdStrike's "Vice President of Marketing," is "knowledgeable about the marketing" of the Accused Products, and lives "in Bee Cave near Austin."[10]

[6] *See* https://www.crowdstrike.com/partners/channel-partners/ (last visited May 15, 2024).

[7] *See, e.g., Webroot, Inc. v. CrowdStrike, Inc.*, Case No. 6:22-cv-00241, Dkt. 59 at 1 (W.D. Tex. Sept. 7, 2022).

[8] *Id.* at 3-4.

[9] *Id.* at 4.

[10] *Id.*

14. On information and belief, CrowdStrike has committed acts of infringement within this District. For example, on information and belief, CrowdStrike uses the Accused Products in this District in manners that practice the Asserted Patents.

15. On information and belief, Defendants make, use, advertise, offer for sale, and/or sell endpoint security software (including the Accused Products) and provide security services that practice the Asserted Patents in the State of Texas and in this District directly and/or through its partnership with businesses in the State of Texas and in this District.

16. On information and belief, Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users.

17. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) because, upon information and belief, Defendants have regular and systematic contacts within this District, have their principal executive offices in this District, and have committed acts of infringement within this District.

## FACTUAL BACKGROUND

### A. GoSecure's Invention of the Asserted Patents

18. GoSecure is a privately held company incorporated in 2004 for the purpose of developing and commercializing products and services protecting customers from cyberattacks.

19. NeuralIQ, the assignee named on the face of the '697 Patent, was initially founded in 2004. In 2011, NeuralIQ relaunched as CounterTack, the assignee named on the face of the '872 Patent. CounterTack acquired GoSecure in 2018 and the company became known as GoSecure, the assignee of record of both Asserted Patents.

20. Today, GoSecure continues to provide Endpoint Detection and Response ("EDR") products and services using the techniques described in the Asserted Patents, including its flagship Titan® Platform, to customers.

21. GoSecure's predecessor, NeuralIQ, filed U.S. Provisional Application No. 61/358,367 on June 24, 2010 ("Provisional Application"). Both Asserted Patents claim priority to the Provisional Application.

22. At the time, the data security industry was focused on identifying and neutralizing malware and viruses using intrusion detection systems (IDS) and intrusion protection systems (IPS) that were predicated on the use of a library of known fingerprints for previously identified malware. For example, such conventional systems could monitor network traffic (e.g., using low-level Internet Protocol (IP) data packets) and compare in-bound packets to a library of fingerprints of malware payloads. Upon detecting a match, the IDS/IPS would be able to take corrective action, such as by preventing further access to the malware.

23. GoSecure, recognizing that attacks would become more sophisticated and that such conventional antivirus software would no longer be able to protect endpoint computers that were accessible via the Internet, developed innovative techniques for defending against sophisticated cyberattacks and obtained over a dozen patents for its technology.

24. For example, GoSecure developed innovative techniques for identifying and responding to so-called "zero-day attacks," against which then-existing IDS/IPS were ineffective. GoSecure recognized that zero-day attacks were able to exploit previously unknown security vulnerabilities, such that there was no malware fingerprint that conventional IDS/IPS could use to detect and thwart such attacks. Accordingly, GoSecure developed and patented techniques,

including those described in the Asserted Patents, for identifying unauthorized activities on a computer system.

### B. CrowdStrike's Pre-Suit Knowledge of the Asserted Patents

25. CrowdStrike was co-founded in or around 2011 by Mr. George Kurtz and Mr. Dmitri Alperovitch. Before founding CrowdStrike, Mr. Kurtz and Mr. Alperovitch met while they were both employed by McAfee, Inc. ("McAfee").

26. In the fall of 2010, Mr. Kurtz asked his assistant at McAfee to arrange a visit for him to GoSecure's offices in Santa Monica, California, purportedly to engage in a technical discussion regarding the future of the cybersecurity industry. Over the course of that visit, which took place in or around November 2010, Mr. Kurtz received detailed technical information about GoSecure's innovative EDR technology. Mr. Kurtz was impressed by GoSecure's technology and even initially expressed interest in serving on GoSecure's Board of Directors and assuming a managerial role at the company.

27. However, Mr. Kurtz joined the Board of Bromium, another start-up in the cybersecurity industry that sought to protect computers through the use of micro-virtualization isolation techniques and the like. Thereafter, Mr. Kurtz rejected offers from GoSecure to join its Board, because he believed his role at Bromium would provide a conflict.

28. Meanwhile, as part of continued efforts to commercialize its innovative technology, GoSecure began seeking investment from venture capitalists and continued to look for additional talented, knowledgeable individuals to serve on its Board of Directors. On September 20, 2011, one of the venture capital investors in GoSecure introduced another McAfee employee, Mr. Dmitri Alperovitch, to GoSecure.

29. Following that introduction, Mr. Alperovitch expressed how impressed he was with GoSecure's technology, claiming that GoSecure was an extremely interesting opportunity and very relevant technology for the evolving cyber threat environment. In or around November 2011, Mr. Alperovitch began serving as a member of GoSecure's Board of Directors, a position he held until May 2012.[11]

30. Shortly before accepting a position on GoSecure's Board of Directors (i.e., in or around September 2011), Mr. Alperovitch resigned from his role as Vice President, Threat Research at McAfee. Unbeknownst to GoSecure, Mr. Alperovitch and Mr. Kurtz intended for CrowdStrike to provide offerings that would compete with GoSecure's technology.

31. To that end, Mr. Alperovitch spent his time on GoSecure's Board of Directors gathering information about GoSecure's technology. Mr. Alperovitch even recommended that GoSecure hire Mr. Jeremy Gould, an engineer with whom Mr. Alperovitch had worked at McAfee, to a senior engineering position at GoSecure in or around December 2011.

32. Mr. Gould worked at GoSecure for multiple months, during which he had broad access to GoSecure's code repository and worked closely with GoSecure's other engineers. However, Mr. Gould quickly soured on the opportunity and became vocal about his discontent, ultimately leaving GoSecure in March 2012, at which point he immediately accepted a position as a senior engineer at CrowdStrike.

33. During his time on GoSecure's Board of Directors, Mr. Alperovitch attended numerous Board meetings at which he received detailed information regarding GoSecure's technology and patent applications, including regarding the claims of the patent application that ultimately issued as the '697 Patent.

[11] Ex. 3 (D. Alperovitch LinkedIn Profile).

34. In or around May 2012—after Mr. Alperovitch had spent six months gathering confidential information while "serving" on GoSecure's Board of Directors—GoSecure sensed there was a conflict of interest and asked Mr. Alperovitch to step down from the Board. While Mr. Alperovitch attributed his decision to a change in GoSecure's strategy to move into the endpoint security market, GoSecure's strategy had been to move into the endpoint security market since before Mr. Alperovitch's first introduction to GoSecure.

35. After Mr. Alperovitch left GoSecure, he continued working at CrowdStrike as its chief technology officer until 2020.

36. On information and belief, Mr. Alperovitch and CrowdStrike have known of the existence of the Asserted Patents since August 11, 2015 ('697 Patent) and April 24, 2018 ('872 Patent).

37. Additionally or alternatively, CrowdStrike has been willfully blind regarding the existence of the Asserted Patents. CrowdStrike closely monitors the technology offerings and intellectual property of other EDR providers, as evidenced by CrowdStrike's website, which advertises comparisons with other companies.[12] On information and belief, to the extent CrowdStrike did not actually know about the existence of the Asserted Patents, CrowdStrike's ignorance was based on its own willful blindness to GoSecure's foundational EDR technology that pre-dated CrowdStrike's incorporation.

38. In April 2023, after being sued by OpenText for patent infringement, and recognizing the foundational nature of GoSecure's technology, CrowdStrike served a subpoena on GoSecure related to prior art products and related documentation that GoSecure had sold beginning

[12] https://www.crowdstrike.com/compare/ (last visited May 15, 2024); *see also* https://sourceforge.net/software/compare/CrowdStrike-Falcon-vs-GoSecure/ (last visited May 15, 2024).

as early as April 2013. In its efforts to invalidate the patents asserted against it, CrowdStrike also cited U.S. Publication No. 2011/0321166, which is a publication of the application that issued as the ’697 Patent, as a prior art reference in the associated *inter partes* review on October 31, 2022.

## THE ASSERTED PATENTS

### A. U.S. Patent No. 9,954,872

39. The ’872 Patent is entitled “System and method for identifying unauthorized activities on a computer system using a data structure model,” and was issued on April 24, 2018, to inventors Alen Capalik, David Andrews, and Ben Becker. GoSecure owns the entire right, title, and interest in and to the ’872 Patent, a copy of which is attached to this Complaint as Exhibit 1.

40. Prior to the ’872 Patent, prior art systems suffered significant drawbacks, especially with respect to protecting networked computers against attacks, unwanted intrusions, and unauthorized access. ’872 Patent at 1:52-57. Network security systems at the time typically resorted to a firewall to prevent unauthorized access. *Id.* at 1:61-63. For example, those prior art intrusion detection and prevention systems relied on a library of malware fingerprints to detect attempts to access computer systems without authorization. *Id.* at 1:63-67. When a connection was attempted to a network port, such systems would compare the in-bound packets to a library of fingerprints; if a match was identified, the systems prevented further access. *Id.* at 2:2-8. But those systems remained vulnerable to so-called zero-day attacks, where there is no known malware fingerprint available for detection. *Id.* at 2:9-17.

41. The ’872 Patent discloses and claims a specific and inventive technical solution that overcomes this particular technological problem in the realm of cyberthreat detection. *Id.* at 2:27-31. The invention provides methods for performing behavioral analysis directly on an endpoint device, using locally-monitored data, to detect, identify, and prevent malicious activities in a way that existing systems could not. *Id.* at 2:29-31. Claim 1 of the ’872 Patent includes limitations

that, alone or in combination, are directed to inventive concepts that were unconventional and not well-known or routine at the time of the inventions. For example, claim 1 recites "monitoring activity on the first computer system" and "identifying… an activity source, an activity target, and an association between the activity source and the activity target," and "storing… a data structure that identifies the activity sources, the activity targets, and the associations,: and "transmitting …information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks" to other computer systems in the network.. *Id.* at Claim 1.

42. Additional claims require limitations that, alone or in combination, are directed to inventive concepts that also were unconventional and not well-known or routine, such as "monitoring all activity on the first computer system" (claim 2); "creating, from the stored information, a fingerprint indicative of the activity on the first computer system" (claim 3); "graphically displaying at least a subset of the stored activities" (claim 7); "identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target" (claim 10); and "identifying activity sources that are affected by unauthorized activities" (claim 12) by, for example, "identifying activity sources that request to execute underprivileged instructions" (claim 14). Unlike the prior art, which failed to protect against zero-day attacks on networked devices, the '872 Patent provides capabilities to identify and transmit to other computers information identifying the zero-day attacks that have no known malware fingerprints.

### B. U.S. Patent No. 9,106,697

43. The ’697 Patent is entitled “System and method for identifying unauthorized activities on a computer system using a data structure model,” and was issued on August 11, 2015, to inventors Alen Capalik, David Andrews, and Ben Becker. GoSecure owns the entire right, title, and interest in and to the ’697 Patent, a copy of which is attached to this Complaint as Exhibit 2.

44. The ’697 Patent also provides techniques for protecting devices against zero-day unauthorized activities and discloses and claims a technical solution that overcomes a specific technological problem in the realm of cyberthreat detection. Claim 1 of the ’697 Patent includes limitations that, alone or in combination, are directed to inventive concepts that were unconventional and not well-known or routine at the time of the inventions. For example, claim 1 recites a computer-implemented method that includes “identifying a plurality of activities being performed at the virtual machine, wherein each of the activities include an activity source, an activity target, and an association between the activity source and the activity target” and “creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine” and “transmitting the fingerprint” to other devices. ’697 Patent at Claim 1. Additional claims require limitations that, alone or in combination, are directed to inventive concepts that also were unconventional and not well-known or routine, such as “monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized” (claim 2); “identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target” (claim 11); and “identifying a type of the association between the activity source and the activity target” (claim

22). Unlike the prior art, which failed to protect zero-day attacks on virtual machines, the ’697 Patent advantageously provides efficient and comprehensive detection and protection.

## CLAIMS FOR PATENT INFRINGEMENT

45. CrowdStrike makes, offers, sells, and uses multiple products that provide and implement malware detection, endpoint protection, and cloud security solutions for individuals and enterprises, each of which incorporate GoSecure’s patented technologies without authorization.

46. For example, CrowdStrike’s Falcon Platform is a cloud-based endpoint protection platform that integrates anti-malware technologies, risk management, and attack forensics to protect remotely connected computers.[13]

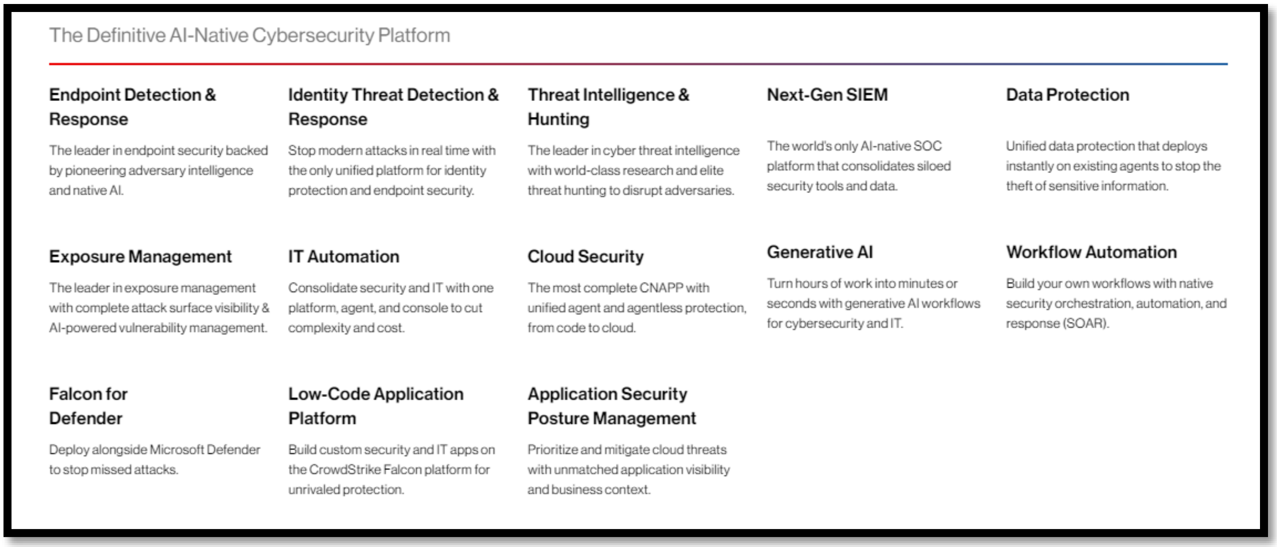
47. CrowdStrike instructs its customers to install the Falcon Platform by downloading the Falcon agent to one or more endpoint devices, which can be things like workstations, desktops, laptops, and other traditional end user computer devices, servers, virtual machines, cloud containers, cloud networks, mobile computer devices such as smartphones, and Internet of Things devices.[14]

48. As shown in the figure below, CrowdStrike’s Falcon Platform includes multiple modules that operate both on endpoint devices and through the cloud using the Falcon agent.[15] These modules are part of and can be added to the base Falcon Platform. Examples of these modules are discussed further below.

[13] *See* https://www.crowdstrike.com/products/ (last visited May 15, 2024).

[14] *See* https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/ (last visited May 15, 2024).

[15] *See* https://www.crowdstrike.com/platform/ (last visited May 15, 2024).



The Definitive AI-Native Cybersecurity Platform

**Endpoint Detection & Response**
The leader in endpoint security backed by pioneering adversary intelligence and native AI.

**Identity Threat Detection & Response**
Stop modern attacks in real time with the only unified platform for identity protection and endpoint security.

**Threat Intelligence & Hunting**
The leader in cyber threat intelligence with world-class research and elite threat hunting to disrupt adversaries.

**Next-Gen SIEM**
The world's only AI-native SOC platform that consolidates siloed security tools and data.

**Data Protection**
Unified data protection that deploys instantly on existing agents to stop the theft of sensitive information.

**Exposure Management**
The leader in exposure management with complete attack surface visibility & AI-powered vulnerability management.

**IT Automation**
Consolidate security and IT with one platform, agent, and console to cut complexity and cost.

**Cloud Security**
The most complete CNAPP with unified agent and agentless protection, from code to cloud.

**Generative AI**
Turn hours of work into minutes or seconds with generative AI workflows for cybersecurity and IT.

**Workflow Automation**
Build your own workflows with native security orchestration, automation, and response (SOAR).

**Falcon for Defender**
Deploy alongside Microsoft Defender to stop missed attacks.

**Low-Code Application Platform**
Build custom security and IT apps on the CrowdStrike Falcon platform for unrivaled protection.

**Application Security Posture Management**
Prioritize and mitigate cloud threats with unmatched application visibility and business context.

49. By way of example, CrowdStrike's Falcon Insight XDR is an endpoint detection and response solution, providing continuous monitoring of endpoint activity and detection, response, and forensics to suspicious activity and malware attacks.[16]

50. Falcon Prevent is a cloud-native Next Generation Antivirus ("NGAV") software solution that detects and prevents known and unknown malware using tools including machine learning, artificial intelligence, and behavior-based indicators of attack ("IOA").[17]

51. Falcon Firewall Management is a software solution that creates, enforces, and maintains firewall rules and policies.[18]

[16] *See* https://www.crowdstrike.com/platform/endpoint-security/ (last visited May 15, 2024).

[17] *See* https://www.crowdstrike.com/products/endpoint-security/falcon-prevent-antivirus/ (last visited May 15, 2024).

[18] *See* https://www.crowdstrike.com/products/endpoint-security/falcon-firewall-management/ (last visited May 15, 2024).

52. CrowdStrike Threat Graph is the cloud-based "brains behind the Falcon endpoint protection platform." CrowdStrike Threat Graph captures, enriches, analyzes, and stores data from endpoint devices.[19]

53. CrowdStrike's Falcon Counter Adversary Operations is a threat intelligence software solution, including Falcon Adversary OverWatch, Falcon Adversary Intelligence, and Falcon Adversary Intelligence Premium.[20]

54. CrowdStrike's Falcon Cloud Security is a solution for cloud detection and response. The solution includes, but is not limited to, Falcon Cloud Security Posture Management. Under this solution, CrowdStrike partners with cloud ecosystems such as Amazon Web Services, Google Cloud, and Microsoft's Azure.[21]

55. The allegations provided below are exemplary and without prejudice to GoSecure's infringement contentions with respect to the Accused Products.

56. As detailed below, each element of at least one claim of each of the Asserted Patents is literally present in the Accused Products. To the extent that any element is not literally present or practiced, each such element is present or practiced under the doctrine of equivalents.

## COUNT I
## Infringement of the '872 Patent

57. GoSecure realleges and incorporates by reference the allegations set forth in the preceding paragraphs of this Complaint.

[19] *See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf (last visited May 15, 2024).

[20] *See* https://www.crowdstrike.com/platform/threat-intelligence/ (last visited May 15, 2024).

[21] *See* https://www.crowdstrike.com/platform/cloud-security/ (last visited May 15, 2024).

58. CrowdStrike has infringed and continues to infringe one or more claims of the ’872 Patent in violation of 35 U.S.C. § 271(a) by, among other things, its making, testing, and using the Accused Products in the United States, including in this District without the permission, consent, authorization, or license of GoSecure. The Accused Products, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’872 Patent.

59. For example, on information and belief, CrowdStrike performs the claimed method in the United States in an infringing manner as described herein by using the Accused Products to protect its own computer and network operations.

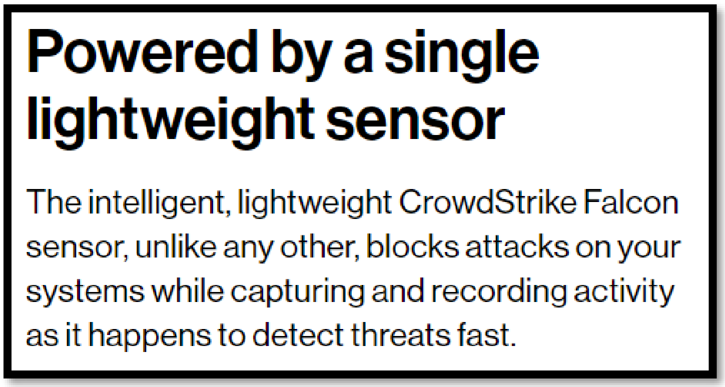
60. On information and belief, CrowdStrike also performs the claimed method in an infringing manner in the United States when testing the Accused Products and corresponding systems and/or when providing or administering services to third parties, customers, and partners using the Accused Products.

61. The Accused Products, when used for their ordinary and customary purpose, meet all the limitations of at least claim 1 of the ’872 Patent. Specifically, claim 1 of the ’872 Patent recites:

> 1. A computer implemented method of identifying unauthorized activities on a first computer system attached to a computer network, wherein the first computer system comprises one or more processors and memory, the method comprising:
>
> monitoring activity on the first computer system;
>
> identifying a plurality of activities being performed at the first computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;
>
> storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and

> transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

62. The Accused Products perform the computer-implemented method of claim 1 of the ’872 Patent because they identify unauthorized activities on a first computer system attached to a computer network, wherein the first computer system comprises one or more processors and memory, as claimed. For example, the Falcon Platform includes an “intelligent, lightweight CrowdStrike Falcon sensor, unlike any other, [that] blocks attacks on your systems while capturing and recording activity as it happens to detect the threats fast.”[22]



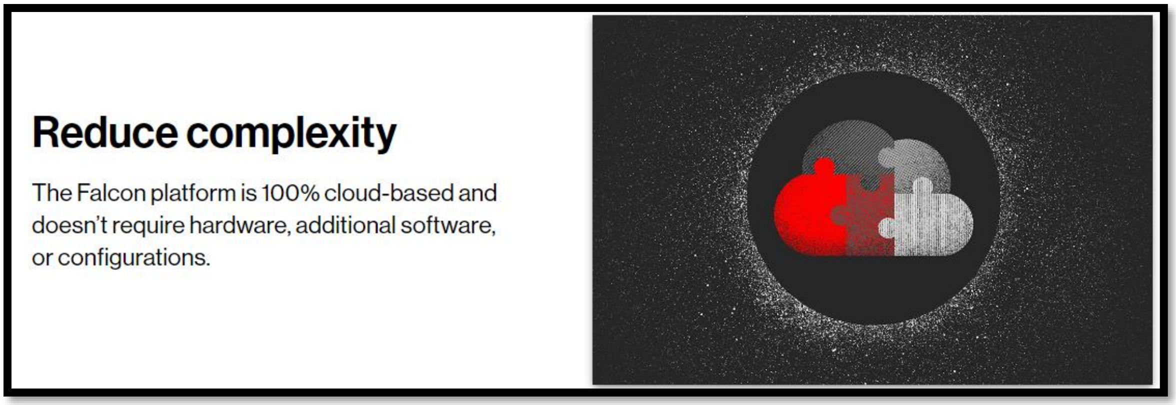
Powered by a single lightweight sensor

The intelligent, lightweight CrowdStrike Falcon sensor, unlike any other, blocks attacks on your systems while capturing and recording activity as it happens to detect threats fast.

63. The computer system is attached to a computer network, as “[t]he Falcon platform is 100% cloud-based and doesn’t require hardware, additional software, or configurations.”[23]

[22] *See* https://www.crowdstrike.com/products/trials/try-falcon-prevent/ (last visited May 15, 2024).

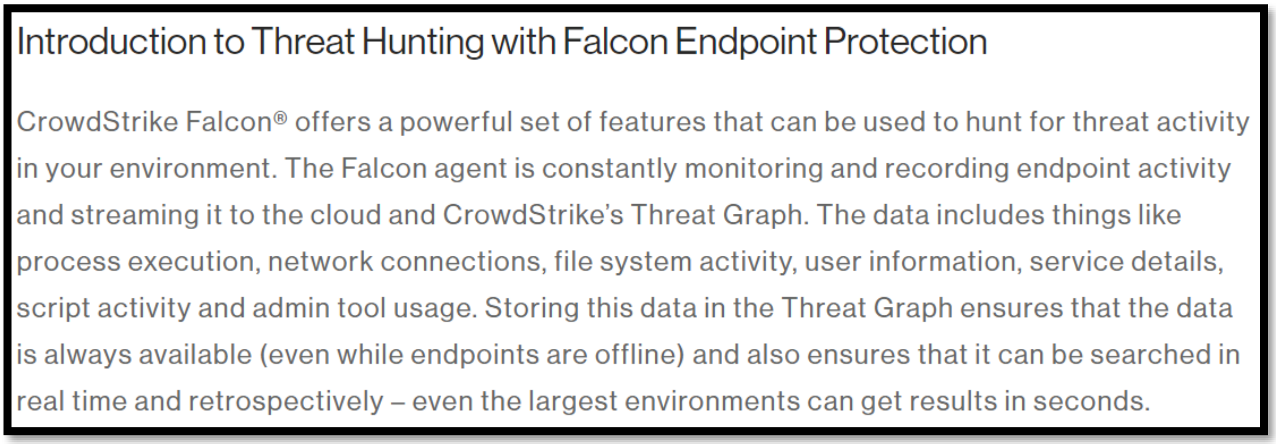
[23] *Id.*



Reduce complexity

The Falcon platform is 100% cloud-based and doesn't require hardware, additional software, or configurations.

64. The method performed by the Accused Products includes monitoring activity on the first computer system. For example, "[t]he Falcon agent is constantly monitoring and recording endpoint activity."[24] Specifically, the data monitored includes "things like process execution, network connections, file system activity, user information, service details, script activity and admin tool usage."[25]



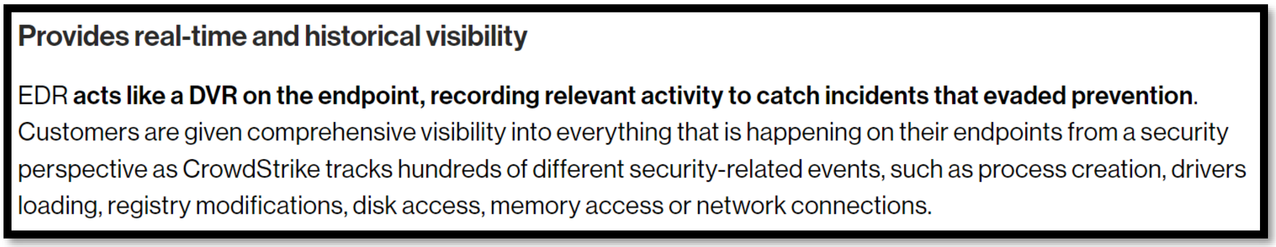
Introduction to Threat Hunting with Falcon Endpoint Protection

CrowdStrike Falcon® offers a powerful set of features that can be used to hunt for threat activity in your environment. The Falcon agent is constantly monitoring and recording endpoint activity and streaming it to the cloud and CrowdStrike's Threat Graph. The data includes things like process execution, network connections, file system activity, user information, service details, script activity and admin tool usage. Storing this data in the Threat Graph ensures that the data is always available (even while endpoints are offline) and also ensures that it can be searched in real time and retrospectively – even the largest environments can get results in seconds.

[24] *See* https://www.crowdstrike.com/blog/tech-center/hunt-threat-activity-falcon-endpoint-protection/ (last visited May 15, 2024).

[25] *Id.*

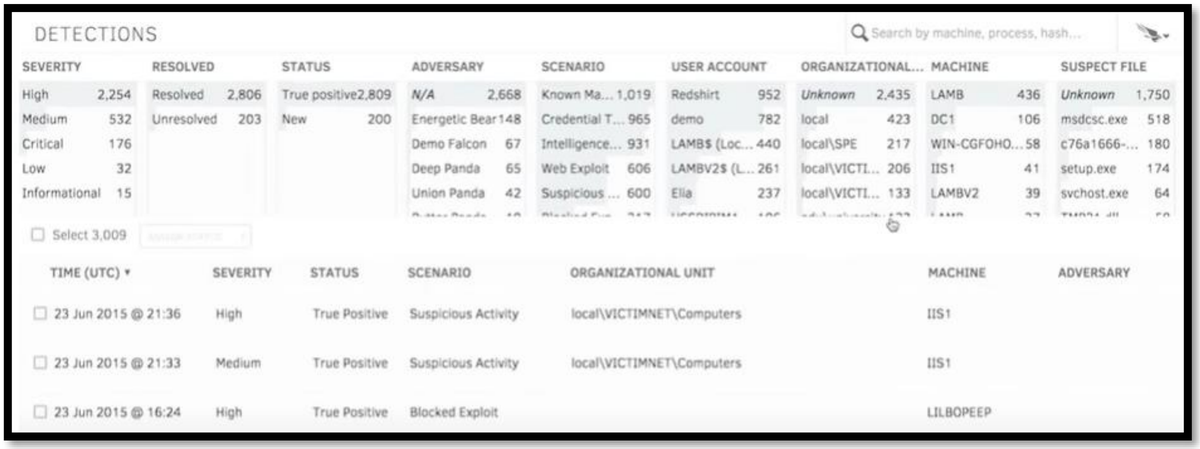
65. Through its use of the Accused Products, CrowdStrike "tracks hundreds of different security-related events, such as process creation, drivers loading, registry modifications, disk access, memory access or network connections."[26]



**Provides real-time and historical visibility**

EDR **acts like a DVR on the endpoint, recording relevant activity to catch incidents that evaded prevention**. Customers are given comprehensive visibility into everything that is happening on their endpoints from a security perspective as CrowdStrike tracks hundreds of different security-related events, such as process creation, drivers loading, registry modifications, disk access, memory access or network connections.

66. The method performed by the Accused Products includes identifying a plurality of activities being performed at the first computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. For example, the Accused Products identify an activity source, activity target, and association, as shown in the example figures below.



DETECTIONS

Search by machine, process, hash...

| SEVERITY | RESOLVED | STATUS | ADVERSARY | SCENARIO | USER ACCOUNT | ORGANIZATIONAL... | MACHINE | SUSPECT FILE |
|---|---|---|---|---|---|---|---|---|
| High 2,254 | Resolved 2,806 | True positive2,809 | *N/A* 2,668 | Known Ma... 1,019 | Redshirt 952 | *Unknown* 2,435 | LAMB 436 | *Unknown* 1,750 |
| Medium 532 | Unresolved 203 | New 200 | Energetic Bear 148 | Credential T... 965 | demo 782 | local 423 | DC1 106 | msdcsc.exe 518 |
| Critical 176 | | | Demo Falcon 67 | Intelligence... 931 | LAMB$ (Loc... 440 | local\SPE 217 | WIN-CGFOHO...58 | c76a1666-... 180 |
| Low 32 | | | Deep Panda 65 | Web Exploit 606 | LAMBV2$ (L... 261 | local\VICTI... 206 | IIS1 41 | setup.exe 174 |
| Informational 15 | | | Union Panda 42 | Suspicious ... 600 | Elia 237 | local\VICTI... 133 | LAMBV2 39 | svchost.exe 64 |

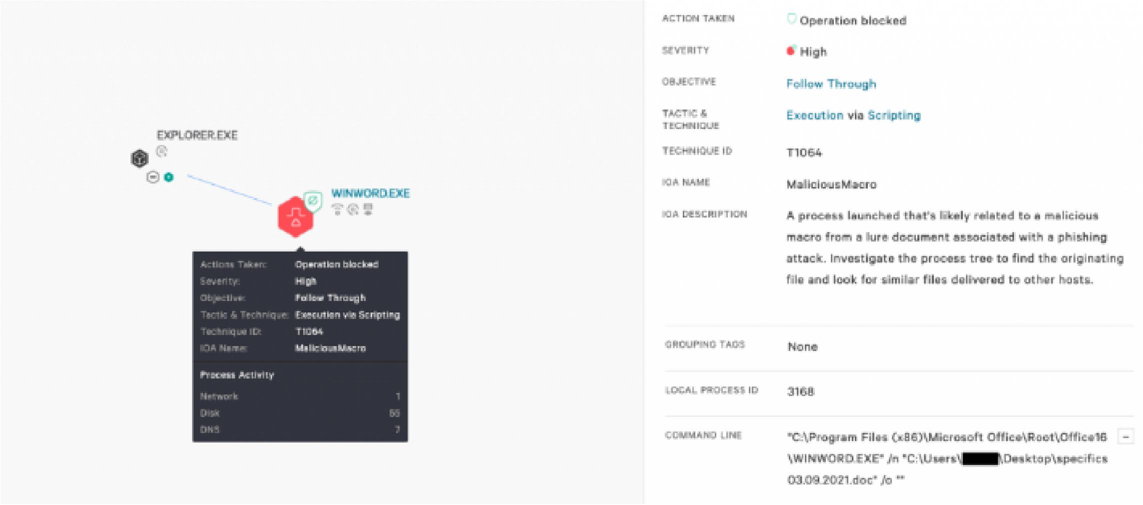
□ Select 3,009

| TIME (UTC) ▾ | SEVERITY | STATUS | SCENARIO | ORGANIZATIONAL UNIT | MACHINE | ADVERSARY |
|---|---|---|---|---|---|---|
| □ 23 Jun 2015 @ 21:36 | High | True Positive | Suspicious Activity | local\VICTIMNET\Computers | IIS1 | |
| □ 23 Jun 2015 @ 21:33 | Medium | True Positive | Suspicious Activity | local\VICTIMNET\Computers | IIS1 | |
| □ 23 Jun 2015 @ 16:24 | High | True Positive | Blocked Exploit | | LILBOPEEP | |

[27]

[26] *See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (last visited May 15, 2024).

[27] *See* https://www.youtube.com/watch?v=tgryLPiVGLE (screenshot at 4:45) (last visited May 15, 2024).



| | |
|---|---|
| Actions Taken: | Operation blocked |
| Severity: | High |
| Objective: | Follow Through |
| Tactic & Technique: | Execution via Scripting |
| Technique ID: | T1064 |
| IOA Name: | MaliciousMacro |

Process Activity

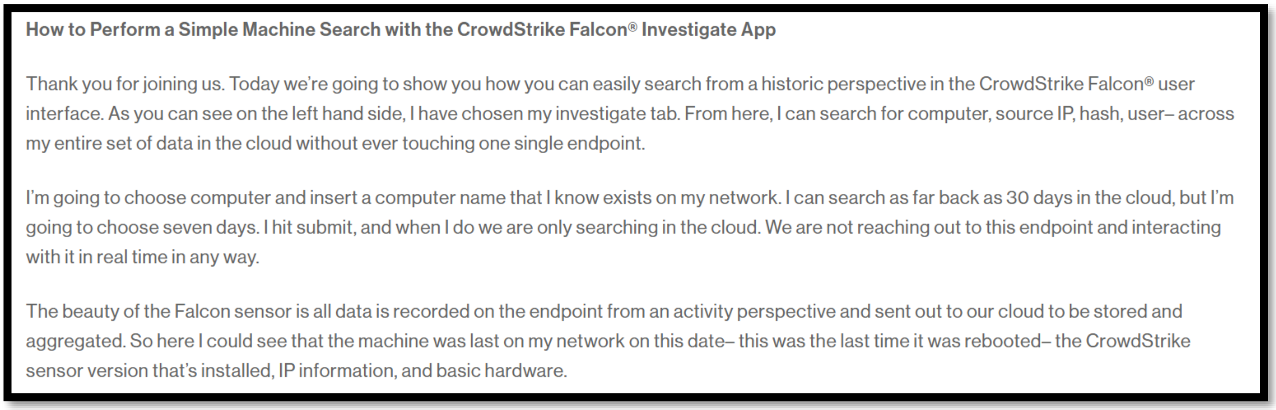
| | |
|---|---|
| Network | 1 |
| Disk | 55 |
| DNS | 7 |

| | |
|---|---|
| ACTION TAKEN | Operation blocked |
| SEVERITY | High |
| OBJECTIVE | Follow Through |
| TACTIC & TECHNIQUE | Execution via Scripting |
| TECHNIQUE ID | T1064 |
| IOA NAME | MaliciousMacro |
| IOA DESCRIPTION | A process launched that's likely related to a malicious macro from a lure document associated with a phishing attack. Investigate the process tree to find the originating file and look for similar files delivered to other hosts. |
| GROUPING TAGS | None |
| LOCAL PROCESS ID | 3168 |
| COMMAND LINE | "C:\Program Files (x86)\Microsoft Office\Root\Office16 \WINWORD.EXE" /n "C:\Users\[redacted]\Desktop\specifics 03.09.2021.doc" /o "" |

Figure 6. Falcon will prevent the malicious BokBot document when the macro executes, thanks to the extended visibility offered by Script-Based Execution Monitoring (Click to enlarge)

[28]

67. The method performed by the Accused Products includes storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities. For example, "[t]he beauty of the Falcon sensor is all data is recorded on the endpoint from an activity perspective."[29]



**How to Perform a Simple Machine Search with the CrowdStrike Falcon® Investigate App**

Thank you for joining us. Today we're going to show you how you can easily search from a historic perspective in the CrowdStrike Falcon® user interface. As you can see on the left hand side, I have chosen my investigate tab. From here, I can search for computer, source IP, hash, user– across my entire set of data in the cloud without ever touching one single endpoint.

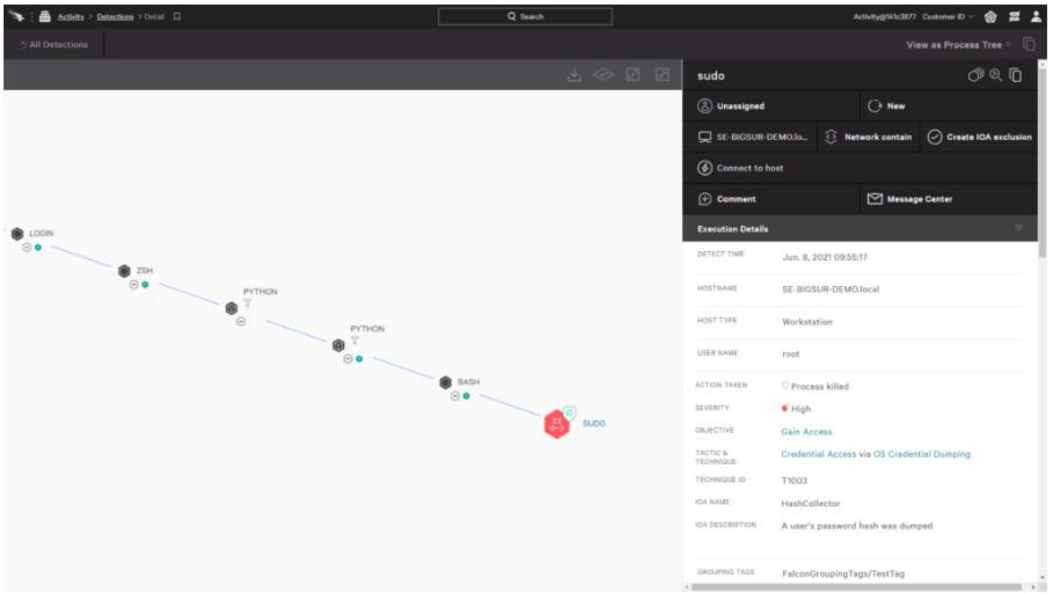
I'm going to choose computer and insert a computer name that I know exists on my network. I can search as far back as 30 days in the cloud, but I'm going to choose seven days. I hit submit, and when I do we are only searching in the cloud. We are not reaching out to this endpoint and interacting with it in real time in any way.

The beauty of the Falcon sensor is all data is recorded on the endpoint from an activity perspective and sent out to our cloud to be stored and aggregated. So here I could see that the machine was last on my network on this date– this was the last time it was rebooted– the CrowdStrike sensor version that's installed, IP information, and basic hardware.

[28] *See* https://www.crowdstrike.com/blog/blocking-fileless-script-based-attacks-using-falcon-script-control-feature/ (last visited May 15, 2024).

[29] *See* https://www.crowdstrike.com/resources/videos/perform-simple-machine-search-crowdstrike-falcon-investigate-app/ (screenshot of transcript) (last visited May 15, 2024).

68. Additionally, when the Accused Products have no internet connection, "the Falcon agent will protect the system and event details will be cached on the endpoint until connectivity is re-established."[30]



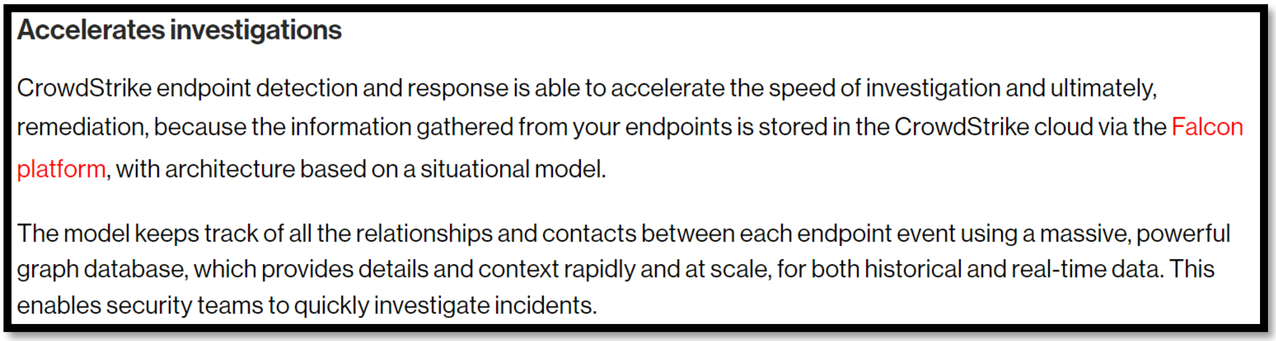
DETECT TIME Jun. 8, 2021 09:55:17
HOSTNAME SE-BIGSUR-DEMO.local
HOST TYPE Workstation
USER NAME root
ACTION TAKEN Process killed
SEVERITY High
OBJECTIVE Gain Access
TACTIC & TECHNIQUE Credential Access via OS Credential Dumping
TECHNIQUE ID T1003
IOA NAME HashCollector
IOA DESCRIPTION A user's password hash was dumped
GROUPING TAGS FalconGroupingTags/TestTag

If there is no internet connectivity at the time of the malicious event, the Falcon agent will protect the system and event details will be cached on the endpoint until connectivity is re-established.

69. The method performed by the Accused Products includes transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations. The Accused Products transmit the collected information

[30] *See* https://www.crowdstrike.com/blog/tech-center/offline-protection/ (last visited May 15, 2024).

(including the activity sources, targets, and associations) to other computer systems, as shown in the figure below.[31]

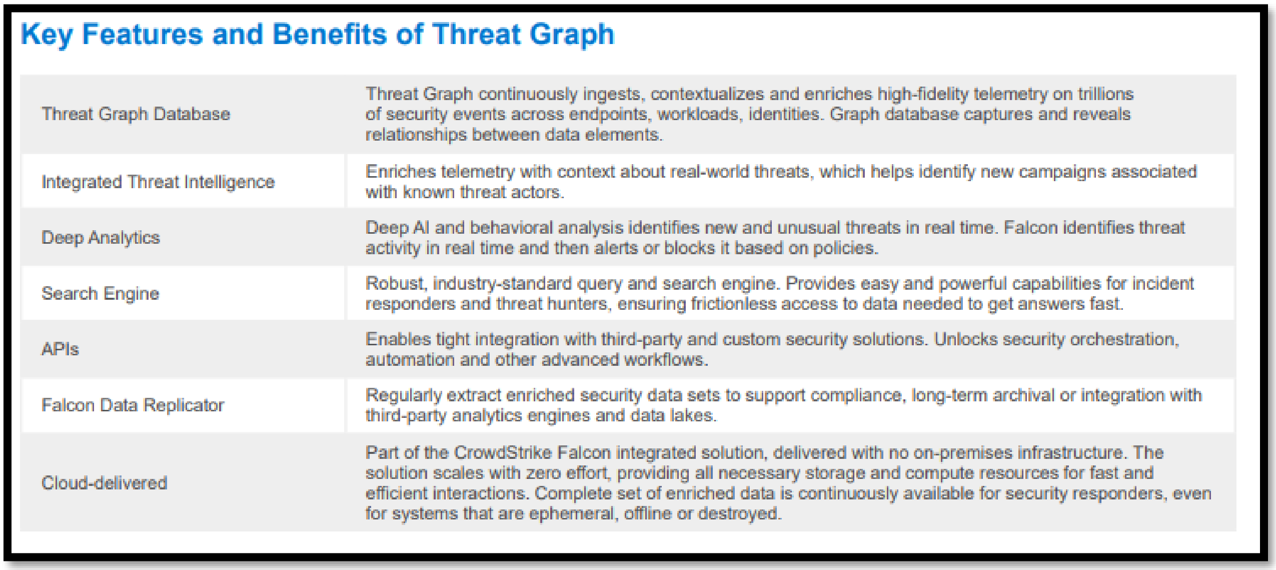


**Accelerates investigations**

CrowdStrike endpoint detection and response is able to accelerate the speed of investigation and ultimately, remediation, because the information gathered from your endpoints is stored in the CrowdStrike cloud via the Falcon platform, with architecture based on a situational model.

The model keeps track of all the relationships and contacts between each endpoint event using a massive, powerful graph database, which provides details and context rapidly and at scale, for both historical and real-time data. This enables security teams to quickly investigate incidents.

70. As another example, the Falcon Threat Graph "continuously ingests, contextualizes and enriches high-fidelity telemetry on trillions of security events across endpoints, workloads, identities."[32]



**Key Features and Benefits of Threat Graph**

| | |
|---|---|
| Threat Graph Database | Threat Graph continuously ingests, contextualizes and enriches high-fidelity telemetry on trillions of security events across endpoints, workloads, identities. Graph database captures and reveals relationships between data elements. |
| Integrated Threat Intelligence | Enriches telemetry with context about real-world threats, which helps identify new campaigns associated with known threat actors. |
| Deep Analytics | Deep AI and behavioral analysis identifies new and unusual threats in real time. Falcon identifies threat activity in real time and then alerts or blocks it based on policies. |
| Search Engine | Robust, industry-standard query and search engine. Provides easy and powerful capabilities for incident responders and threat hunters, ensuring frictionless access to data needed to get answers fast. |
| APIs | Enables tight integration with third-party and custom security solutions. Unlocks security orchestration, automation and other advanced workflows. |
| Falcon Data Replicator | Regularly extract enriched security data sets to support compliance, long-term archival or integration with third-party analytics engines and data lakes. |
| Cloud-delivered | Part of the CrowdStrike Falcon integrated solution, delivered with no on-premises infrastructure. The solution scales with zero effort, providing all necessary storage and compute resources for fast and efficient interactions. Complete set of enriched data is continuously available for security responders, even for systems that are ephemeral, offline or destroyed. |

[31] *See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (last visited May 15, 2024).

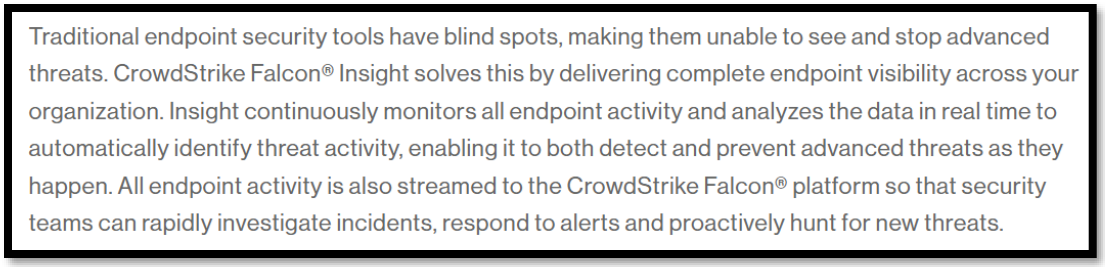
[32] *See* https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/technical-support/crowdstrike-threat-graph-datasheet.pdf (last visited May 15, 2024).

71. The Accused Products, when used for their ordinary and customary purpose, additionally meet all the limitations of various dependent claims of the ’872 Patent. For example, claims 2, 3, 7, 10, 12, and 14 of the ’872 Patent recite:

> 2. The method of claim 1, wherein the monitoring further comprises monitoring all activity on the first computer system.
>
> 3. The method of claim 1, further comprising:
>
> creating, from the stored information, a fingerprint indicative of the activity on the first computer system.
>
> 7. The method of claim 1, further comprising:
>
> graphically displaying at least a subset of the stored activities.
>
> 10. The method of claim 1, further comprising:
>
> identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.
>
> 12. The method of claim 1, further comprising:
>
> identifying activity sources that are affected by unauthorized activities.
>
> 14. The method of claim 12, wherein:
>
> instructions executed by the one or more processors have respective privilege levels;
>
> respective activity sources have respective privilege levels; and
>
> the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions.

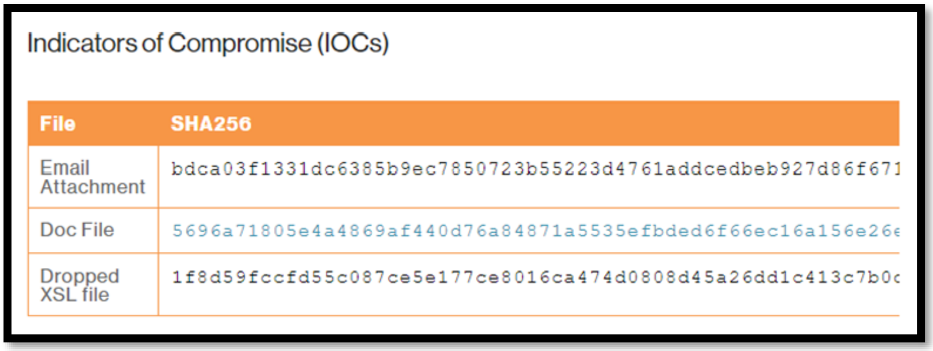
72. The Accused Products perform the computer-implemented method of claim 2 of the ’872 Patent because they monitor all activity on the computer system. For example, “[Falcon] Insight continuously monitors all endpoint activity and analyzes the data in real time to

automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen.”[33]



Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon® Insight solves this by delivering complete endpoint visibility across your organization. Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

73. The Accused Products perform the computer-implemented method of claim 3 of the ’872 Patent because they create, from the stored information, a fingerprint indicative of the activity on the first computer system. For example, the Falcon Platform uses the stored information to generate indicators of compromise (“IOCs”), or hashes, that can be used for future detection.[34]



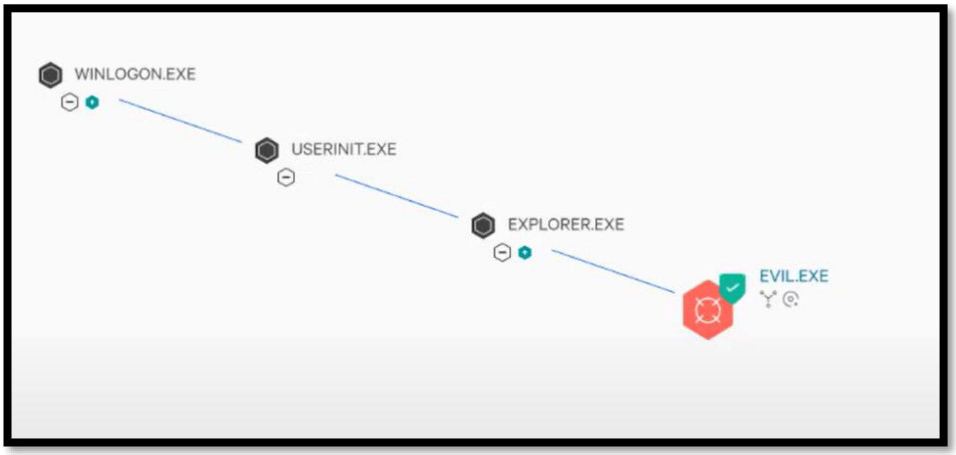
Indicators of Compromise (IOCs)

| File | SHA256 |
|---|---|
| Email Attachment | bdca03f1331dc6385b9ec7850723b55223d4761addcedbeb927d86f671 |
| Doc File | 5696a71805e4a4869af440d76a84871a5535efbded6f66ec16a156e26e |
| Dropped XSL file | 1f8d59fccfd55c087ce5e177ce8016ca474d0808d45a26dd1c413c7b0c |

[33] *See* https://www.crowdstrike.com/resources/data-sheets/falcon-insight-xdr/ (last visited May 15, 2024).

[34] *See* https://www.crowdstrike.com/blog/blocking-fileless-script-based-attacks-using-falcon-script-control-feature/ (last visited May 15, 2024).

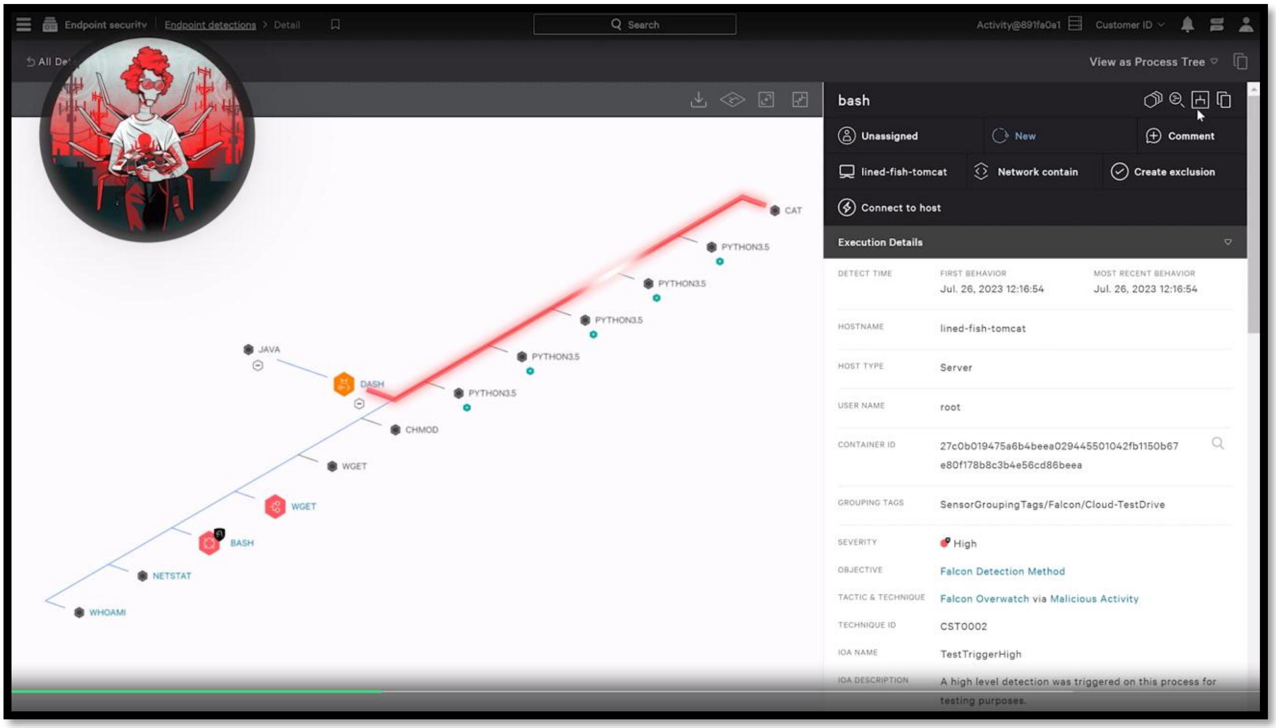
74. The Accused Products perform the computer-implemented method of claim 7 of the ’872 Patent because they graphically display at least a subset of the stored activities. For example, the Falcon Platform graphically displays to users the activity it identified and recorded.[35]



75. The Accused Products perform the computer-implemented method of claim 10 of the ’872 Patent because they identify a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.[36]

[35] *See* https://www.youtube.com/watch?v=4B4a5FQZ8dE&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs&t=20s (screenshot at 0:35) (last visited May 15, 2024).

[36] *See* https://www.crowdstrike.com/products/cloud-security/cloud-security-posture-management-cspm/ (last visited May 15, 2024).



DETECT TIME
FIRST BEHAVIOR Jul. 26, 2023 12:16:54
MOST RECENT BEHAVIOR Jul. 26, 2023 12:16:54

HOSTNAME lined-fish-tomcat

HOST TYPE Server

USER NAME root

CONTAINER ID 27c0b019475a6b4beea029445501042fb1150b67e80f178b8c3b4e56cd86beea

GROUPING TAGS SensorGroupingTags/Falcon/Cloud-TestDrive

SEVERITY High

OBJECTIVE Falcon Detection Method

TACTIC & TECHNIQUE Falcon Overwatch via Malicious Activity

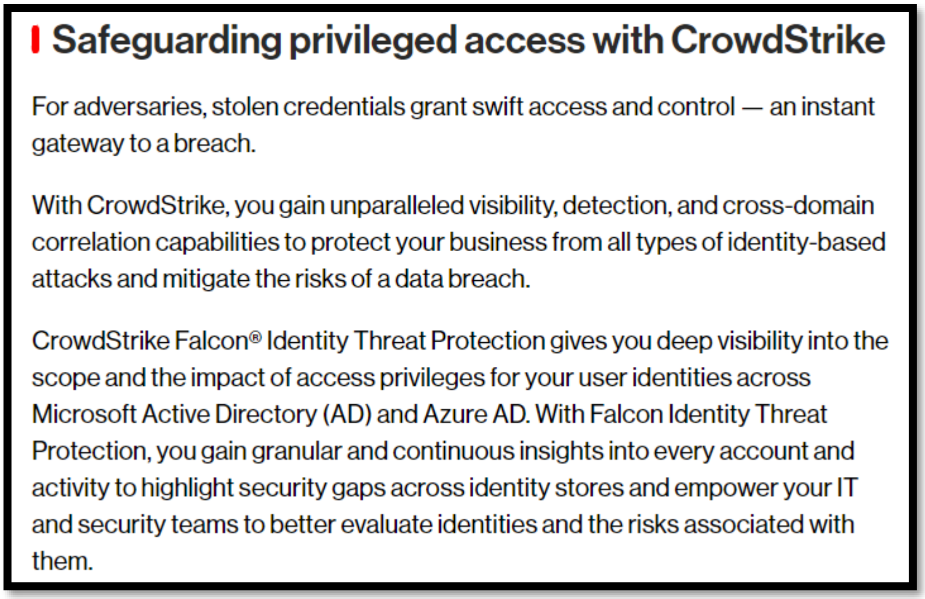
TECHNIQUE ID CST0002

IOA NAME TestTriggerHigh

IOA DESCRIPTION A high level detection was triggered on this process for testing purposes.

76. The Accused Products perform the computer-implemented method of claims 12 and 14 of the ’872 Patent because they identify activity sources that are affected by unauthorized activities, and instructions executed by the one or more processors have respective privilege levels, the respective activity sources have respective privilege levels, and the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions. For example, “CrowdStrike Falcon® Identity Threat Protection gives you deep visibility into the scope and the impact of access privileges for your user identities across Microsoft Active Directory (AD) and Azure AD.”[37]

[37] *See* https://www.crowdstrike.com/cybersecurity-101/what-is-privileged-access-management/ (last visited May 15, 2024).



Safeguarding privileged access with CrowdStrike

For adversaries, stolen credentials grant swift access and control — an instant gateway to a breach.

With CrowdStrike, you gain unparalleled visibility, detection, and cross-domain correlation capabilities to protect your business from all types of identity-based attacks and mitigate the risks of a data breach.

CrowdStrike Falcon® Identity Threat Protection gives you deep visibility into the scope and the impact of access privileges for your user identities across Microsoft Active Directory (AD) and Azure AD. With Falcon Identity Threat Protection, you gain granular and continuous insights into every account and activity to highlight security gaps across identity stores and empower your IT and security teams to better evaluate identities and the risks associated with them.

77. In addition to directly infringing the ’872 Patent, as discussed above, CrowdStrike knew or was willfully blind to the fact that it was inducing infringement of at least claim 1 of the ’872 Patent under 35 U.S.C. § 271(b) by instructing, encouraging, directing, and requiring third parties to directly infringe by performing the method of at least claim 1 in the United States. CrowdStrike instructs its customers regarding how to install and operate the Accused Products in an infringing manner, including by providing user guides and customer support.

78. As discussed above, CrowdStrike, by and through at least Mr. Alperovitch, knew about GoSecure’s patented technology by no later than February 2012. On information and belief, CrowdStrike knew about (or was willfully blind to) the ’872 Patent by no later than April 24, 2018, i.e., its date of issuance. CrowdStrike further knows about the ’872 Patent from its receipt of this Complaint.

79. CrowdStrike is also liable for contributory infringement of at least claim 1 of the ’872 Patent under 35 U.S.C. § 271(c) by knowing or being willfully blind to the fact that it was contributing to infringement by providing to its customers and offering to sell and selling in the United States the Accused Products.

80. The Accused Products are software that perform the method of at least claim 1 of the ’872 Patent when installed on a computer device having at least one processor and memory and are not a staple article or commodity of commerce suitable for substantial noninfringing use. Specifically, as described above, the Accused Products infringe the computer-implemented method of claim 1 when they are installed on a compatible computer containing a processor and memory and used for their intended purpose within the United States.

81. CrowdStrike has known of the existence of the ’872 Patent, and its acts of infringement have been knowing, intentional, and willful (or willfully blind) and in disregard for the ’872 Patent, without any reasonable basis for believing that it had a right to engage in the infringing conduct.

82. CrowdStrike’s acts of infringement of the ’872 Patent have injured and continue to injure GoSecure in an amount to be proven at trial, but not less than a reasonable royalty. GoSecure has suffered and continues to suffer damages, including lost profits, as a result of CrowdStrike’s infringement of the ’872 Patent.

83. CrowdStrike’s infringement has caused and is continuing to cause damage and irreparable harm to GoSecure, and GoSecure will continue to suffer damage and irreparable harm unless and until that infringement is enjoined by this Court.

84. This case is exceptional and, therefore, GoSecure is entitled to an award of increased damages under 35 U.S.C. § 284, and attorney’s fees and costs incurred under 35 U.S.C. § 285.

## COUNT II
## Infringement of the ’697 Patent

85. GoSecure realleges and incorporates by reference the allegations set forth in the preceding paragraphs of this Complaint.

86. CrowdStrike has infringed and continues to infringe one or more claims of the ’697 Patent in violation of 35 U.S.C. § 271(a) by, among other things, its making, testing, and using the Accused Products in the United States, including in this District without the permission, consent, authorization, or license of GoSecure. The Accused Products, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’697 Patent.

87. For example, on information and belief, CrowdStrike performs the claimed method in an infringing manner as described herein by using the Accused Products in the United States to protect its own computer and network operations.

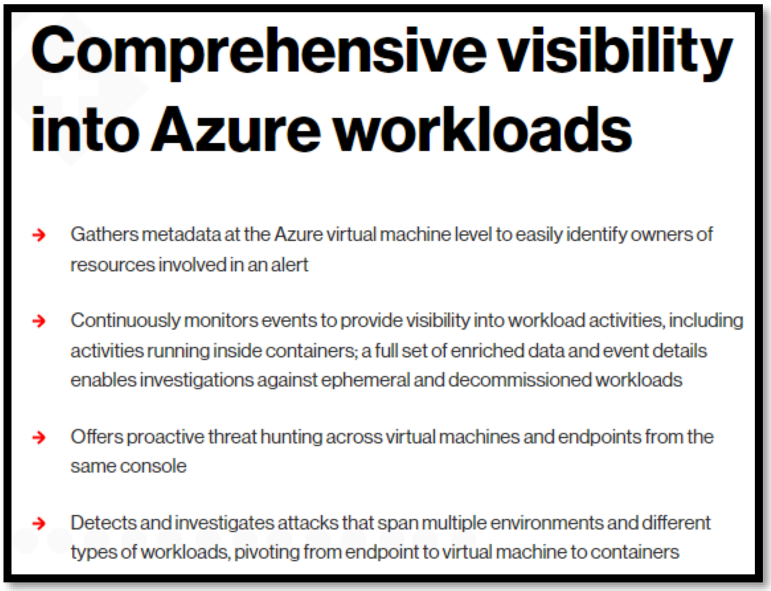
88. On information and belief, CrowdStrike also performs the claimed method in an infringing manner when testing the Accused Products and corresponding systems in the United States and/or when providing or administering services to third parties, customers, and partners using the Accused Products in the United States.

89. The Accused Products meet all the limitations of at least claim 1 of the ’697 Patent. Specifically, claim 1 of the ’697 Patent recites:

> 1. A computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises:
>
> one or more processors; and memory storing: a virtual machine; and a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor:
>
> monitoring activity on the virtual machine;
>
> identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;
>
> storing in the memory the activity sources, activity targets, and associations;

> creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and
>
> transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

90. The Accused Products perform the computer-implemented method of claim 1 of the ’697 Patent because they identify unauthorized activities on a computer system attached to a computer network. For example, Falcon Cloud Security for Azure “[g]athers metadata at the Azure virtual machine level to easily identify owners of resources involved in an alert,” and “[c]ontinuously monitors events to provide visibility into workload activities, including activities running inside containers.”[38]



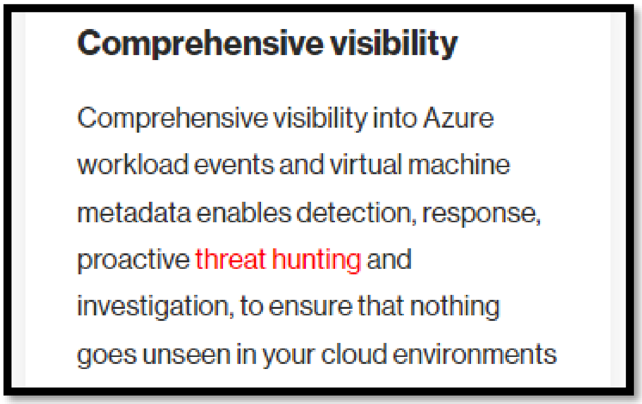
## Comprehensive visibility into Azure workloads

- → Gathers metadata at the Azure virtual machine level to easily identify owners of resources involved in an alert
- → Continuously monitors events to provide visibility into workload activities, including activities running inside containers; a full set of enriched data and event details enables investigations against ephemeral and decommissioned workloads
- → Offers proactive threat hunting across virtual machines and endpoints from the same console
- → Detects and investigates attacks that span multiple environments and different types of workloads, pivoting from endpoint to virtual machine to containers

91. The Accused Products identify unauthorized activities as they provide “[c]omprehensive visibility into Azure workload events and virtual machine metadata enables

[38] *See* https://www.crowdstrike.com/products/cloud-security/falcon-for-azure/ (last visited May 15, 2024).

detection, response, proactive threat hunting and investigation, to ensure that nothing goes unseen in your cloud environments."[39]



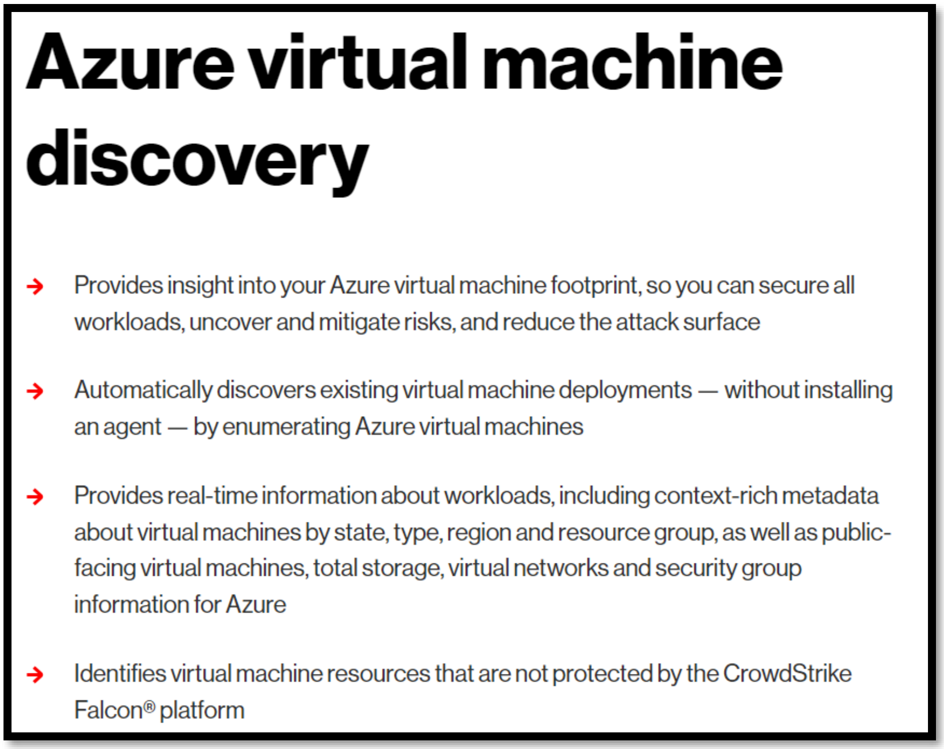
**Comprehensive visibility**

Comprehensive visibility into Azure workload events and virtual machine metadata enables detection, response, proactive threat hunting and investigation, to ensure that nothing goes unseen in your cloud environments

92. The computer-implemented method performed by the Accused Products includes the use of one or more processors and memory storing a virtual machine and a virtual machine monitor supervising the virtual machine. For example, the Accused Products "[p]rovide[] insight into your Azure virtual machine footprint, so you can secure all workloads, uncover and mitigate risks, and reduce the attack surface."[40]

[39] *Id.*

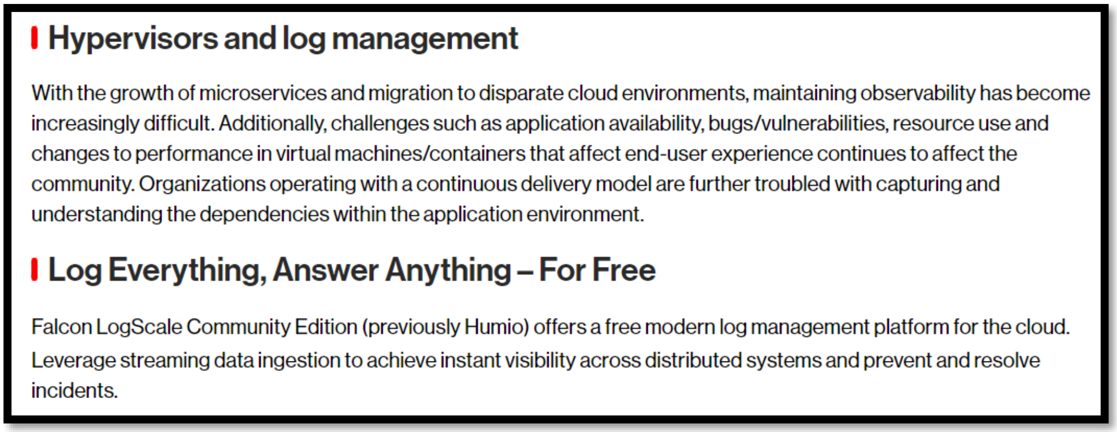
[40] *Id.*



## Azure virtual machine discovery

- Provides insight into your Azure virtual machine footprint, so you can secure all workloads, uncover and mitigate risks, and reduce the attack surface
- Automatically discovers existing virtual machine deployments — without installing an agent — by enumerating Azure virtual machines
- Provides real-time information about workloads, including context-rich metadata about virtual machines by state, type, region and resource group, as well as public-facing virtual machines, total storage, virtual networks and security group information for Azure
- Identifies virtual machine resources that are not protected by the CrowdStrike Falcon® platform

93. In addition, the Accused Products include "hypervisors," which are also known as virtual machine monitors that are used to supervise virtual machines.[41]



### Hypervisors and log management

With the growth of microservices and migration to disparate cloud environments, maintaining observability has become increasingly difficult. Additionally, challenges such as application availability, bugs/vulnerabilities, resource use and changes to performance in virtual machines/containers that affect end-user experience continues to affect the community. Organizations operating with a continuous delivery model are further troubled with capturing and understanding the dependencies within the application environment.

### Log Everything, Answer Anything – For Free

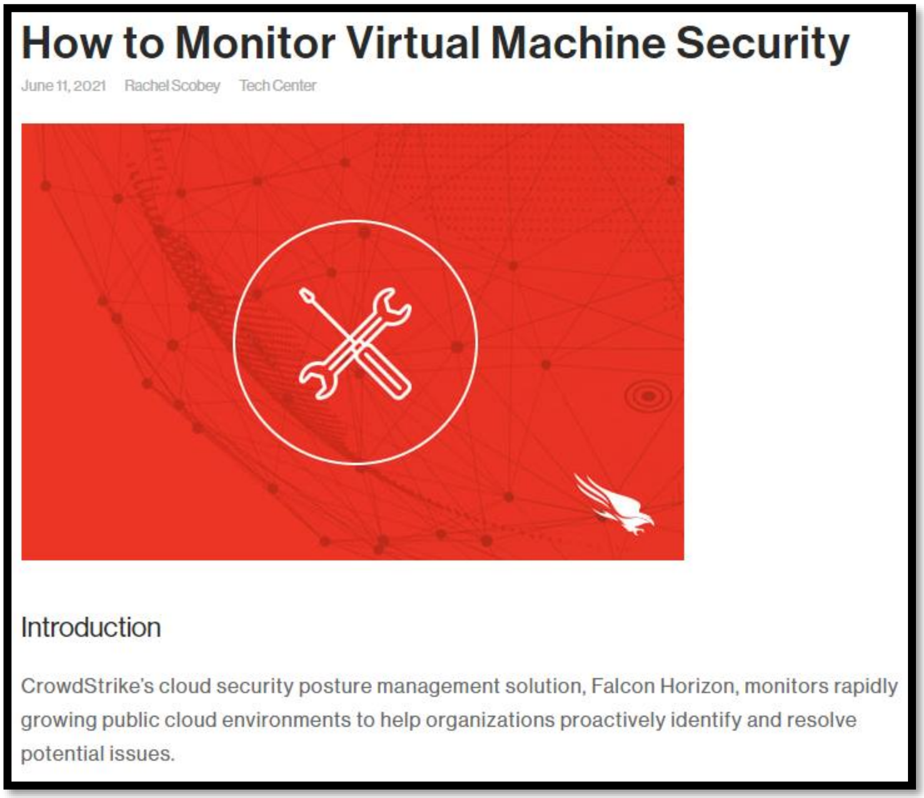
Falcon LogScale Community Edition (previously Humio) offers a free modern log management platform for the cloud. Leverage streaming data ingestion to achieve instant visibility across distributed systems and prevent and resolve incidents.

94. The method performed by the Accused Products includes monitoring activity on the virtual machine. For example, as described above, the Accused Products "[c]ontinuously

[41] *See* https://www.crowdstrike.com/cybersecurity-101/observability/hypervisors-vmm/ (last visited May 15, 2024).

monitor[] events to provide visibility into workload activities, including activities running inside containers; a full set of enriched data and event details enables investigations against ephemeral and decommissioned workloads."[42]

95. As another example of infringing activity performed by the Accused Products, Falcon Horizon, which is CrowdStrike's Falcon Cloud Security Posture Management solution, "monitors rapidly growing public cloud environments to help organizations proactively identify and resolve potential issues."[43]



How to Monitor Virtual Machine Security

June 11, 2021 Rachel Scobey Tech Center

Introduction

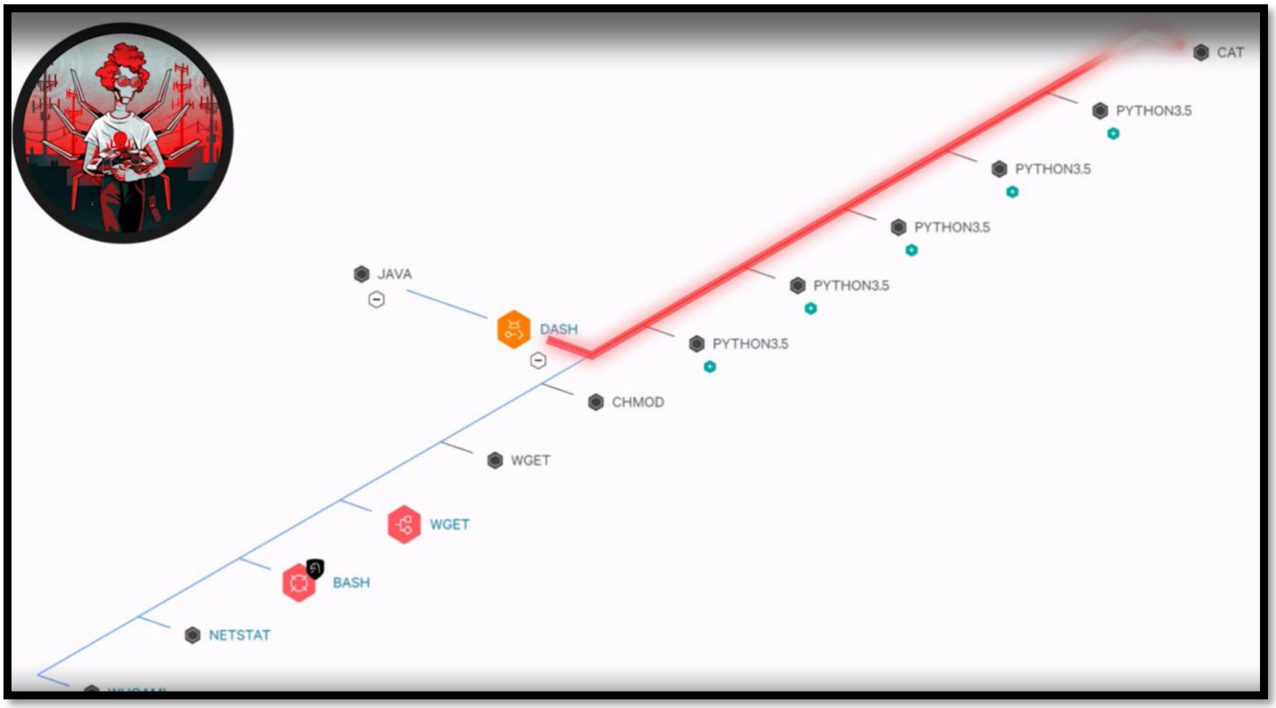
CrowdStrike's cloud security posture management solution, Falcon Horizon, monitors rapidly growing public cloud environments to help organizations proactively identify and resolve potential issues.

96. The method performed by the Accused Products includes identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity

[42] *See* https://www.crowdstrike.com/products/cloud-security/falcon-for-azure/ (last visited May 15, 2024).

[43] *See* https://www.crowdstrike.com/blog/tech-center/monitor-virtual-machine/ (last visited May 15, 2024).

source, an activity target, and an association between the activity source and the activity target. By way of example, the figure below demonstrates the activity source, activity target, and association that are identified.[44]

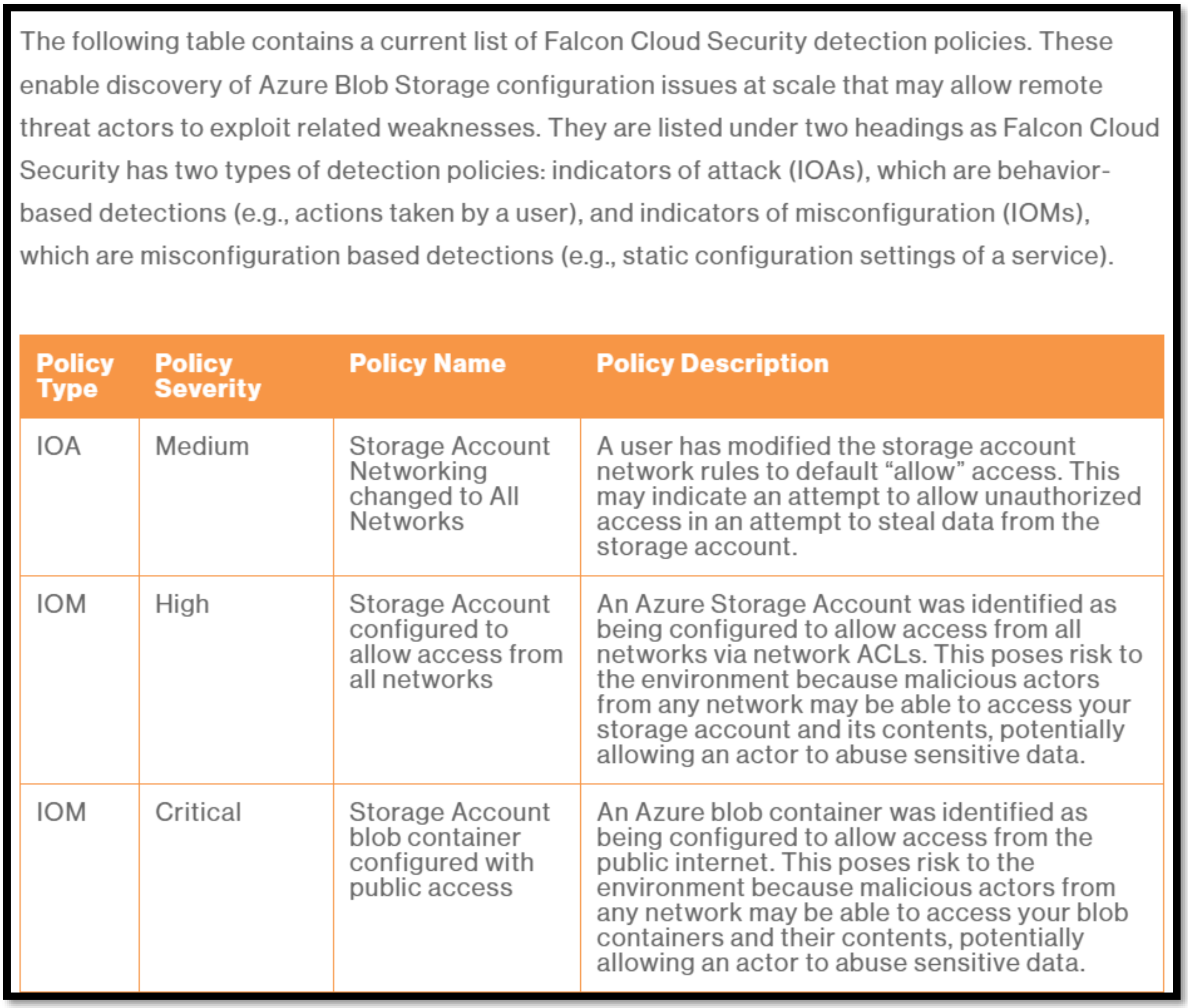


97. The method performed by the Accused Products includes storing in the memory the activity sources, activity targets, and associations. In order for the Accused Products to operate, they must store the identified activities in memory, as the virtual machine and the virtual machine monitor are themselves stored in the memory.

98. The method performed by the Accused Products includes creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine. For example, Falcon Cloud Security may detect based on "indicators of attack (IOAs)" and "indicators of

[44] *See* https://www.crowdstrike.com/products/cloud-security/cloud-security-posture-management-cspm/ (screenshot at 0:37) (last visited May 15, 2024).

misconfiguration (IOMs)," which are policies for detection that will generate IDs for the particular incident.[45]



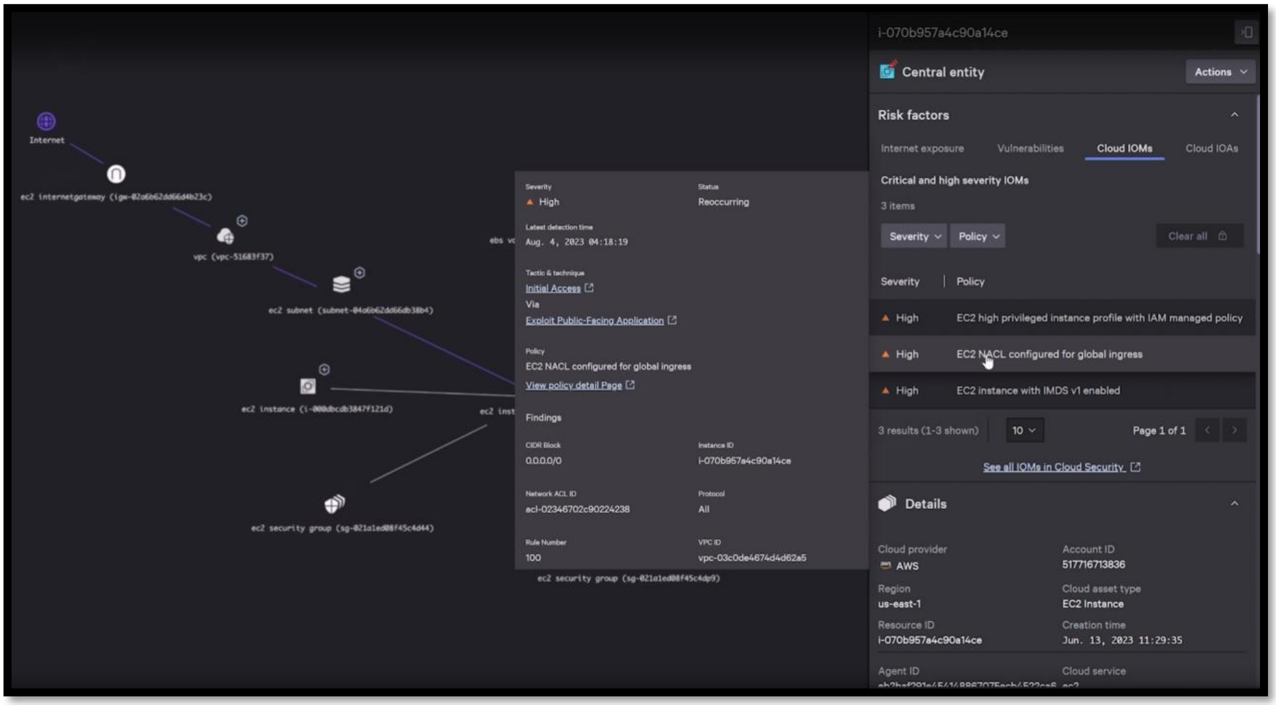
The following table contains a current list of Falcon Cloud Security detection policies. These enable discovery of Azure Blob Storage configuration issues at scale that may allow remote threat actors to exploit related weaknesses. They are listed under two headings as Falcon Cloud Security has two types of detection policies: indicators of attack (IOAs), which are behavior-based detections (e.g., actions taken by a user), and indicators of misconfiguration (IOMs), which are misconfiguration based detections (e.g., static configuration settings of a service).

| Policy Type | Policy Severity | Policy Name | Policy Description |
|---|---|---|---|
| IOA | Medium | Storage Account Networking changed to All Networks | A user has modified the storage account network rules to default "allow" access. This may indicate an attempt to allow unauthorized access in an attempt to steal data from the storage account. |
| IOM | High | Storage Account configured to allow access from all networks | An Azure Storage Account was identified as being configured to allow access from all networks via network ACLs. This poses risk to the environment because malicious actors from any network may be able to access your storage account and its contents, potentially allowing an actor to abuse sensitive data. |
| IOM | Critical | Storage Account blob container configured with public access | An Azure blob container was identified as being configured to allow access from the public internet. This poses risk to the environment because malicious actors from any network may be able to access your blob containers and their contents, potentially allowing an actor to abuse sensitive data. |

99. As shown in the figure below, the "Cloud IOMs" (i.e., indicators of misconfiguration) generates identifiers (e.g., fingerprints) that can identify the particular activity on the virtual machine.[46]

[45] *See* https://www.crowdstrike.com/blog/how-crowdstrike-detects-cloud-storage-misconfigurations/ (last visited May 15, 2024).

[46] *See* https://www.crowdstrike.com/products/cloud-security/cloud-security-posture-management-cspm/ (screenshot at 1:10) (last visited May 15, 2024).


Internet
ec2 internetgateway (igw-02a6b62dd66d4b23c)
vpc (vpc-51683f37)
ec2 subnet (subnet-04a6b62dd66db38b4)
ec2 instance (i-000dbcdb3847f121d)
ec2 security group (sg-021a1ed08f45c4d44)
ebs vc
ec2 inst
ec2 security group (sg-021a1ed08f45c4dp9)

Severity
High

Status
Reoccurring

Latest detection time
Aug. 4, 2023 04:18:19

Tactic & technique
Initial Access
Via
Exploit Public-Facing Application

Policy
EC2 NACL configured for global ingress
View policy detail Page

Findings

CIDR Block
0.0.0.0/0

Instance ID
i-070b957a4c90a14ce

Network ACL ID
acl-02346702c90224238

Protocol
All

Rule Number
100

VPC ID
vpc-03c0de4674d4d62a5

i-070b957a4c90a14ce

Central entity

Actions

Risk factors

Internet exposure | Vulnerabilities | Cloud IOMs | Cloud IOAs

Critical and high severity IOMs

3 items

Severity | Policy | Clear all

| Severity | Policy |
|---|---|
| ▲ High | EC2 high privileged instance profile with IAM managed policy |
| ▲ High | EC2 NACL configured for global ingress |
| ▲ High | EC2 instance with IMDS v1 enabled |

3 results (1-3 shown) 10 Page 1 of 1

See all IOMs in Cloud Security

Details

Cloud provider
AWS

Account ID
517716713836

Region
us-east-1

Cloud asset type
EC2 Instance

Resource ID
i-070b957a4c90a14ce

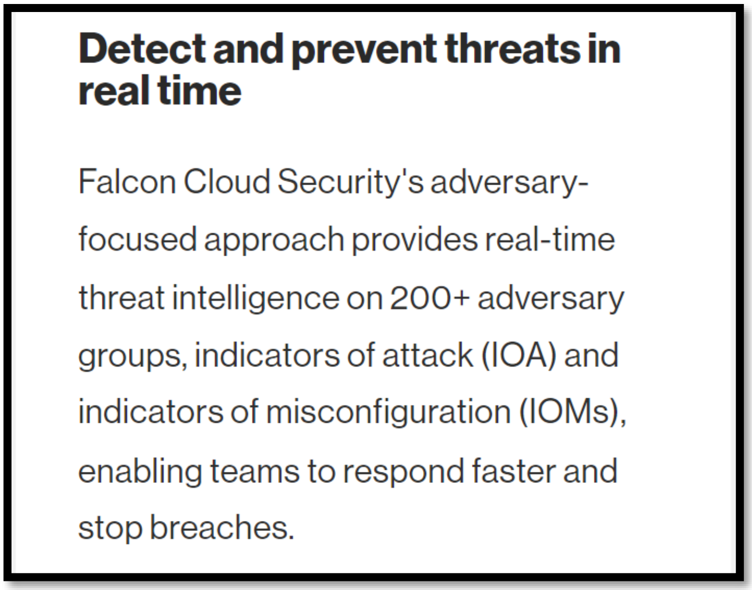
Creation time
Jun. 13, 2023 11:29:35

Agent ID

Cloud service

100. The method performed by the Accused Products includes transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. For example, Falcon Cloud Security "provides real-time threat intelligence on 200+ adversary groups, indicators of attack (IOA) and indicators of misconfiguration (IOMs), enabling teams to respond faster and stop breaches."[47] The Accused Products transmit the fingerprint so that Falcon Cloud Security has on record large numbers of indicators of misconfigurations, which helps to prevent future attacks.

[47] *See* https://www.crowdstrike.com/products/cloud-security/cloud-security-posture-management-cspm/ (last visited May 15, 2024).

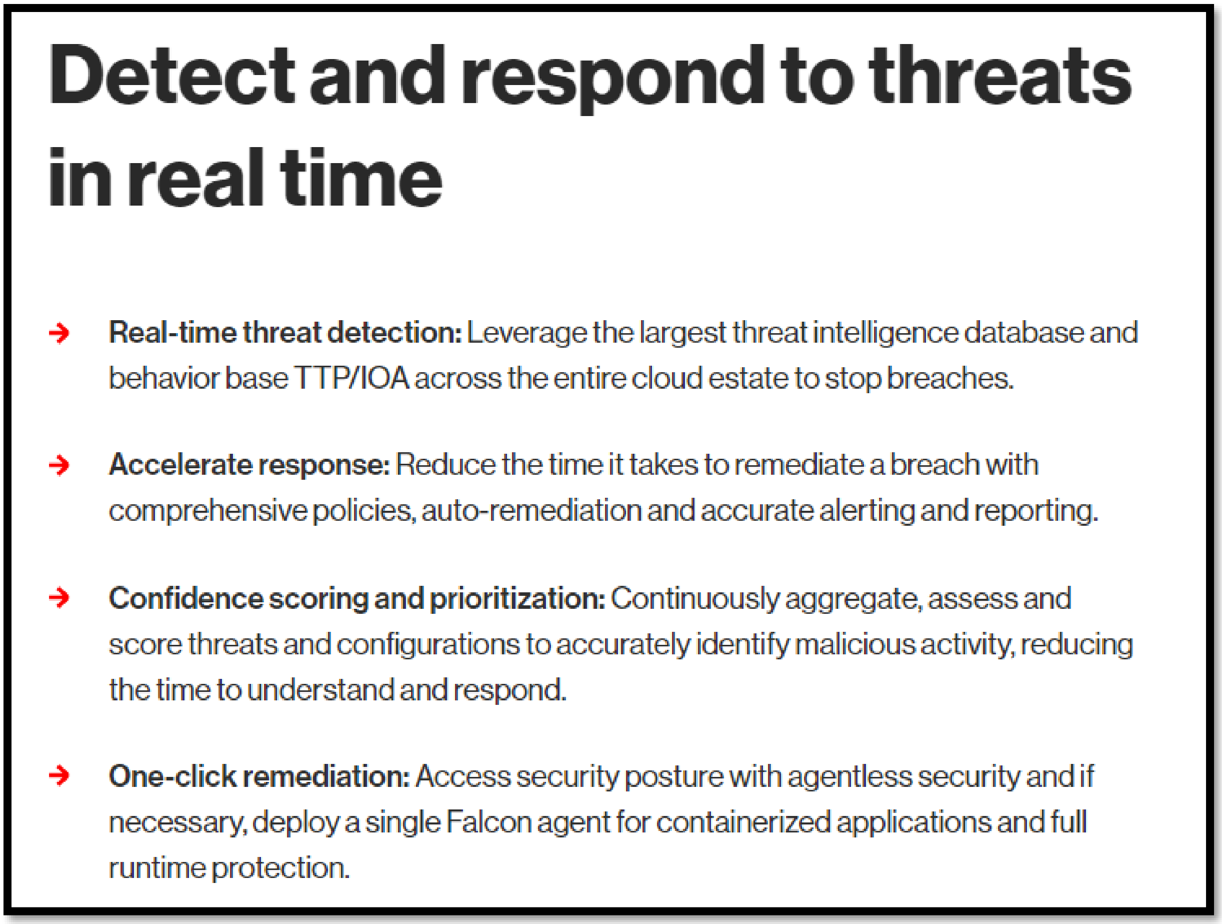


Detect and prevent threats in real time

Falcon Cloud Security's adversary-focused approach provides real-time threat intelligence on 200+ adversary groups, indicators of attack (IOA) and indicators of misconfiguration (IOMs), enabling teams to respond faster and stop breaches.

101. Similarly, the Accused Products maintain "the largest threat intelligence database and behavior base TTP/IOA across the entire cloud estate to stop breaches."[48]

[48] *See* https://www.crowdstrike.com/products/cloud-security/cloud-security-posture-management-cspm/ (last visited May 15, 2024).



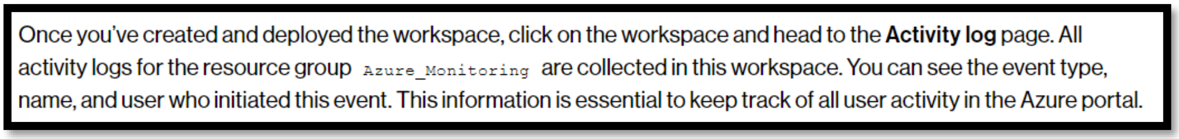
## Detect and respond to threats in real time

- **Real-time threat detection:** Leverage the largest threat intelligence database and behavior base TTP/IOA across the entire cloud estate to stop breaches.
- **Accelerate response:** Reduce the time it takes to remediate a breach with comprehensive policies, auto-remediation and accurate alerting and reporting.
- **Confidence scoring and prioritization:** Continuously aggregate, assess and score threats and configurations to accurately identify malicious activity, reducing the time to understand and respond.
- **One-click remediation:** Access security posture with agentless security and if necessary, deploy a single Falcon agent for containerized applications and full runtime protection.

102. The Accused Products, when used for their ordinary and customary purpose, additionally meet all the limitations of various dependent claims of the ’697 Patent. For example, claims 2, 11, and 22 of the ’697 Patent recite:

> 2. The method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.
>
> 11. The method of claim 1, further comprising identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.
>
> 22. The method of claim 1, further comprising:
>
> identifying a type of the association between the activity source and the activity target.

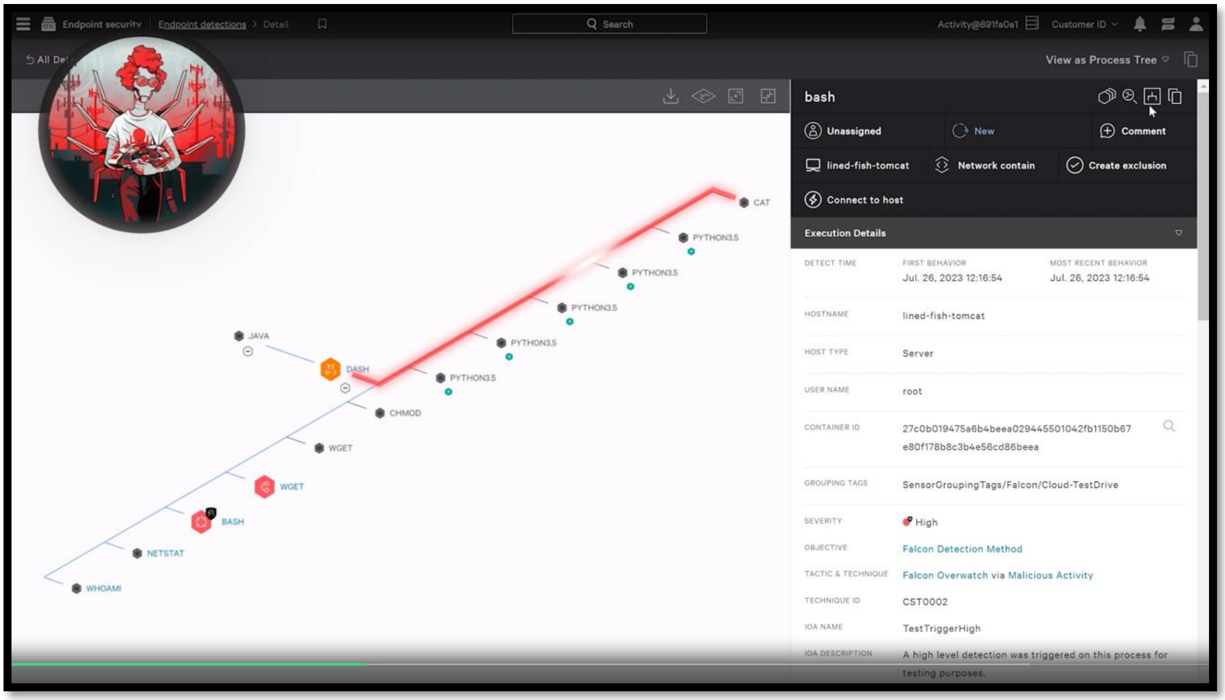
103. The Accused Products perform the computer-implemented method of claim 2 of the ’697 Patent because they monitor all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized. For example, “[a]ll activity logs for the resource group Azure_Monitoring are collected in this workspace. You can see the event type, name, and user who initiated this event. This information is essential to keep track of all user activity in the Azure portal.”[49]


Once you've created and deployed the workspace, click on the workspace and head to the **Activity log** page. All activity logs for the resource group `Azure_Monitoring` are collected in this workspace. You can see the event type, name, and user who initiated this event. This information is essential to keep track of all user activity in the Azure portal.

104. The Accused Products perform the computer-implemented method of claim 11 of the ’697 Patent because they identify a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.[50]

[49] *See* https://www.crowdstrike.com/guides/azure-logging/advanced-concepts/ (last visited May 15, 2024).

[50] *See* https://www.crowdstrike.com/products/cloud-security/cloud-security-posture-management-cspm/ (last visited May 15, 2024).



bash

DETECT TIME — FIRST BEHAVIOR Jul. 26, 2023 12:16:54 — MOST RECENT BEHAVIOR Jul. 26, 2023 12:16:54

HOSTNAME lined-fish-tomcat

HOST TYPE Server

USER NAME root

CONTAINER ID 27c0b019475a6b4beea029445501042fb1150b67e80f178b8c3b4e56cd86beea

GROUPING TAGS SensorGroupingTags/Falcon/Cloud-TestDrive

SEVERITY High

OBJECTIVE Falcon Detection Method

TACTIC & TECHNIQUE Falcon Overwatch via Malicious Activity

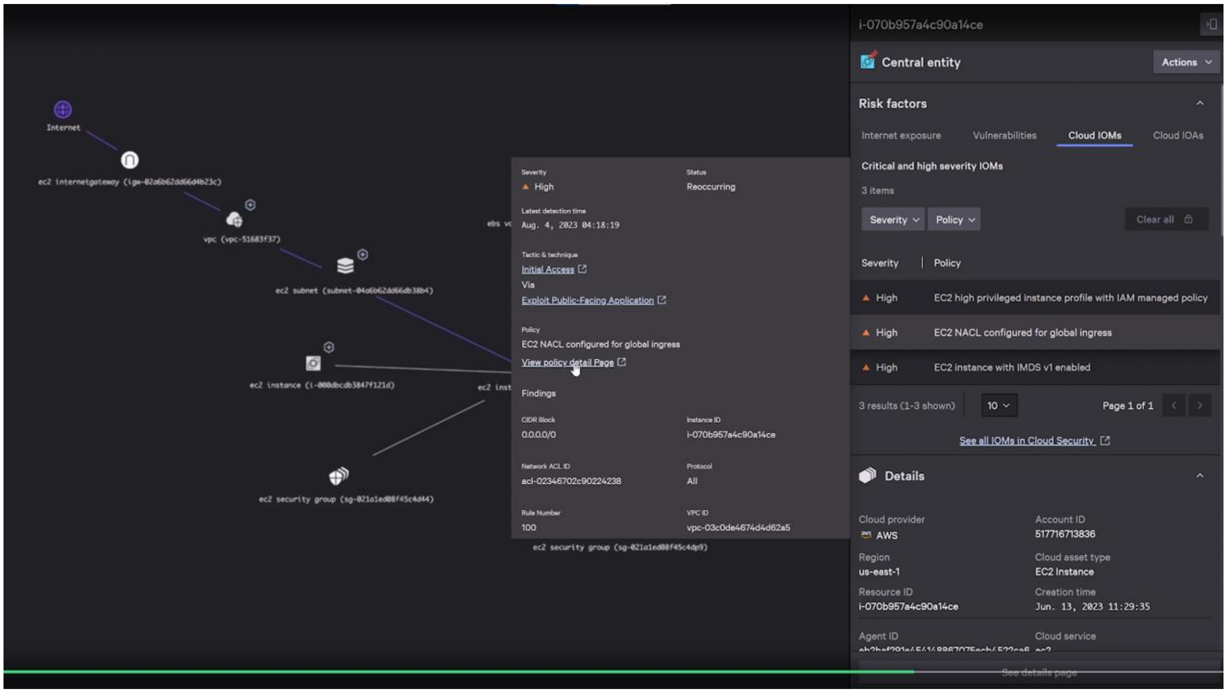
TECHNIQUE ID CST0002

IOA NAME TestTriggerHigh

IOA DESCRIPTION A high level detection was triggered on this process for testing purposes.

105. The Accused Products perform the computer-implemented method of claim 22 of the ’697 Patent because they identify a type of the association between the activity source and the activity target. For example, the Accused Products identify that the following association between the activity source and the activity target to have a “High” severity level.[51]

[51] *See* https://www.crowdstrike.com/products/cloud-security/cloud-security-posture-management-cspm/ (screenshot at 1:10) (last visited May 15, 2024).


Internet
ec2 internetgateway (igw-02a6b62dd66d4b23c)
vpc (vpc-51683f37)
ec2 subnet (subnet-04a6b62dd66db38b4)
ec2 instance (i-000dbcdb3847f121d)
ec2 security group (sg-021a1ed08f45c4d44)
ebs vo
ec2 inst
ec2 security group (sg-021a1ed08f45c4dp9)

Severity
▲ High

Status
Reoccurring

Latest detection time
Aug. 4, 2023 04:18:19

Tactic & technique
Initial Access
Via
Exploit Public-Facing Application

Policy
EC2 NACL configured for global ingress
View policy detail Page

Findings

CIDR Block
0.0.0.0/0

Instance ID
i-070b957a4c90a14ce

Network ACL ID
acl-02346702c90224238

Protocol
All

Rule Number
100

VPC ID
vpc-03c0de4674d4d62a5

i-070b957a4c90a14ce

Central entity

Actions

Risk factors

Internet exposure | Vulnerabilities | Cloud IOMs | Cloud IOAs

Critical and high severity IOMs

3 items

Severity | Policy | Clear all

| Severity | Policy |
|---|---|
| ▲ High | EC2 high privileged instance profile with IAM managed policy |
| ▲ High | EC2 NACL configured for global ingress |
| ▲ High | EC2 instance with IMDS v1 enabled |

3 results (1-3 shown) 10 Page 1 of 1

See all IOMs in Cloud Security

Details

Cloud provider
AWS

Account ID
517716713836

Region
us-east-1

Cloud asset type
EC2 Instance

Resource ID
i-070b957a4c90a14ce

Creation time
Jun. 13, 2023 11:29:35

Agent ID

Cloud service

See details page

106. In addition to directly infringing the ’697 Patent, as discussed above, CrowdStrike knew or was willfully blind to the fact that it was inducing infringement of at least claim 1 of the ’697 Patent under 35 U.S.C. § 271(b) by instructing, encouraging, directing, and requiring third parties to directly infringe by performing the method of at least claim 1 in the United States.

107. As discussed above, CrowdStrike, by and through at least Mr. Alperovitch, knew about GoSecure’s patented technology by no later than February 2012. On information and belief, CrowdStrike knew about or was willfully blind to the ’697 Patent by no later than August 11, 2015, i.e., its date of issuance. Additionally, on information and belief, CrowdStrike knew about or was willfully blind to the ’697 Patent as of October 31, 2022, when CrowdStrike cited U.S. Publication No. 2011/0321166 as a prior art reference in *inter partes* reviews against OpenText. CrowdStrike further knows about the ’697 Patent from its receipt of this Complaint.

108. CrowdStrike is also liable for contributory infringement of at least claim 1 of the ’697 Patent under 35 U.S.C. § 271(c) by knowing or being willfully blind to the fact that it was

contributing to infringement by providing to its customers and offering to sell and selling in the United States the Accused Products.

109. The Accused Products are software that perform the method of at least claim 1 of the ’697 Patent when installed on a computer device having at least one processor and memory and are not a staple article or commodity of commerce suitable for substantial noninfringing use. Specifically, as described above, the Accused Products infringe the computer-implemented method of claim 1 when they are installed on a compatible computer containing a processor and memory and used for their ordinary and customary purpose.

110. CrowdStrike has known of the existence of the ’697 Patent, and its acts of infringement have been knowing, intentional, and willful (or willfully blind) and in disregard for the ’697 Patent, without any reasonable basis for believing that it had a right to engage in the infringing conduct.

111. CrowdStrike’s acts of infringement of the ’697 Patent have injured and continue to injure GoSecure in an amount to be proven at trial, but not less than a reasonable royalty. GoSecure has suffered and continues to suffer damages, including lost profits, as a result of CrowdStrike’s infringement of the ’697 Patent.

112. CrowdStrike’s infringement has caused and is continuing to cause damage and irreparable harm to GoSecure, and GoSecure will continue to suffer damage and irreparable harm unless and until that infringement is enjoined by this Court.

113. This case is exceptional and, therefore, GoSecure is entitled to an award of increased damages under 35 U.S.C. § 284, and attorney’s fees and costs incurred under 35 U.S.C. § 285.

## JURY DEMAND

114. GoSecure demands a jury trial as to all issues that are triable by a jury in this action.

## PRAYER FOR RELIEF

WHEREFORE, GoSecure respectfully prays for relief as follows:

A. Judgment that Defendants are liable for direct infringement, and/or inducing the infringement, and/or contributing to the infringement of one or more claims of each of the Asserted Patents;

B. An Order preliminarily and permanently enjoining Defendants and their respective officers, agents, employees, and those in privity or in active concert or participation with them, from further infringement of the Asserted Patents;

C. Compensatory damages in an amount according to proof, including lost profits, and in any event no less than a reasonable royalty;

D. Increased damages under 35 U.S.C. § 284;

E. Pre-judgment interest;

F. Post-judgment interest;

G. Attorneys' fees based on this being an exceptional case pursuant to 35 U.S.C. § 285, including pre-judgment interest on such fees;

H. An accounting and/or supplemental damages for all damages incurred by Plaintiff from six years prior to the date this lawsuit was filed through entry of a final, non-appealable judgment;

I. If this Court declines to enjoin Defendants from infringing any of the Asserted Patents, damages for future infringement in lieu of an injunction; and

J. Any further relief that the Court deems just and proper.

DATED: May 16, 2024

Respectfully submitted,

*/s/ Giri Pathmanaban*
S. Giri Pathmanaban (SBN: 24074865)
Daniel S. Todd (*pro hac vice to be filed*)
LATHAM AND WATKINS LLP
300 Colorado Street, Suite 2400
Austin, TX 78701
Tel: (737) 910-7300
Giri.Pathmanaban@lw.com
Daniel.Todd@lw.com

Maximilian A. Grant (SBN: 481610)
LATHAM AND WATKINS LLP
555 Eleventh Street, NW, Suite 1000
Washington, D.C. 20004
Tel: (202) 637-2200
Max.Grant@lw.com

Clement Naples (*pro hac vice to be filed*)
LATHAM AND WATKINS LLP
1271 Avenue of the Americas
New York, NY 10020
Tel: (212) 906-1200
Clement.Naples@lw.com

Amit Makker (*pro hac vice to be filed*)
LATHAM AND WATKINS LLP
505 Montgomery Street, Suite 2000
San Francisco, CA 94111
Tel: (415) 391-0600
Amit.Makker@lw.com

**ATTORNEYS FOR PLAINTIFF GOSECURE, INC.**